# CONTENTS

## PART 1

### Getting Started

## CHAPTER 4

**Introduction to Cisco Prime Infrastructure**

- Prime Infrastructure Organization

## CHAPTER 5

**Adding Licenses**

- About Traditional Licenses
- Adding a Traditional License to Access Features
- About the Smart License Feature

## CHAPTER 6

**Adding Devices to Prime Infrastructure**

- Methods for Adding Devices
- Adding Devices Using Discovery
  - Understanding the Discovery Process
  - Running Discovery
  - Running Quick Discovery
  - Verifying Discovery
- Importing Devices from Another Source
- CSV File Requirements for Importing Devices
- Adding Devices Manually
  - Adding Virtual Device Context (VDC) Device
- About Adding Wireless Devices
- Validating That Devices Were Added Successfully
  - Verifying Device Credentials
  - Editing Device Parameters
  - Synchronizing
Adding NAM HTTP/HTTPS Credentials  6-xii
Exporting Devices  6-xiii
Next Steps  6-xiii

CHAPTER 7

Grouping Devices  7-i
   Grouping Devices by Device Type  7-ii

CHAPTER 8

Setting Up Network Monitoring  8-i
   Monitoring Port Groups and Interfaces  8-ii
      Setting Up WAN Interface Monitoring  8-iii
   Getting Enhanced Client Information by Integrating with Cisco Identity Services Engine (ISE)  8-iii
      Adding an Identity Services Engine  8-iv
      Configuring ACS View Servers  8-iv
   Setting Up Assurance for Performance Monitoring  8-iv
      Enabling NAM Data Collection  8-v
      Defining NAM Polling Parameters  8-v
      Enabling NetFlow Data Collection  8-vi

CHAPTER 9

Changing User Settings  9-i
   Setting User Preferences  9-ii
   Changing Your User Preferences  9-ii
   Changing Your Idle-User Timeout  9-ii
   Changing List Length  9-iii

CHAPTER 10

Viewing and Managing Dashboards  10-i
   Types of Dashboards  10-ii
      Network Summary Dashboards  10-ii
      Overview Dashboards  10-iv
      Wireless Dashboards  10-vi
      Performance Dashboards  10-vi
      Data Center Dashboards  10-viii
   Managing and Editing Dashboards  10-ix
Viewing Options for Metrics 10-ix
Understanding Dashlet Icons 10-ix
Adding Dashboards 10-xi
Adding Dashlets 10-xi
  Default Dashlets 10-xi
  Time Filters for Dashboards and Dashlets 10-xvii
  Overriding a Dashlet Filter 10-xvii
  Creating Generic Dashlets 10-xviii
Restoring Dashboards 10-xviii

CHAPTER 11
Troubleshooting Network Health Using Dashboards 11-i
  Defining Health Rules 11-ii
  Network Health Map Features 11-ii
    Network Health Display Options 11-iii
  Network Health Summary 11-iv

PART 1
Monitoring Your Network

CHAPTER 13
Monitoring Devices 13-i
  Monitoring Network Devices 13-ii
    Network Devices Page 13-ii
  Monitoring Jobs 13-ii
  Monitoring Background Tasks 13-iv
  Using Packet Capture to Monitor and Troubleshoot Network Traffic 13-iv
  Securing Network Services 13-v

CHAPTER 14
Monitoring Wireless Devices 14-i
  Monitoring Controllers 14-ii
    Monitoring System Parameters 14-ii
    Spanning Tree Protocol 14-iii
    Management Frame Protection 14-iv
Contents

Rogue AP Rules 14-iv
Monitoring Third Party Controllers 14-v
Monitoring Switches 14-v
Configuring the Switch List Page 14-v
Monitoring Switch System Parameters 14-vi
Monitoring Switch Interfaces 14-vii
Monitoring Switch Clients 14-viii

Monitoring Access Points 14-viii
Searching for Access Points 14-viii
Viewing a List of Access Points 14-ix
Configuring the List of Access Points Display 14-ix
Types of Reports for Access Points 14-x
Generating Reports for Access Points 14-xi
Monitoring Traffic Load 14-xii
Monitoring Dynamic Power Control 14-xii
Monitoring Access Points Noise 14-xii
Monitoring Access Points Interference 14-xiii
Monitoring Access Points Coverage (RSSI) 14-xiii
Monitoring Access Points Coverage (SNR) 14-xiv
Monitoring Access Points Up/Down Statistics 14-xiv
Monitoring the Access Points Voice Statistics 14-xiv
Monitoring the Access Points Voice TSM Table 14-xv
Monitoring the Access Points Voice TSM Reports 14-xv
Monitoring Access Points 802.11 Counters 14-xvi
Monitoring Access Points AP Profile Status 14-xvi
Monitoring Access Points Radio Utilization 14-xvi
Monitoring Access Points Traffic Stream Metrics 14-xvi
Monitoring Access Points Tx Power and Channel 14-xvii
Monitoring VoIP Calls 14-xvii
Monitoring Voice Statistics 14-xvii
Monitoring Air Quality 14-xviii
Monitoring Access Points Details 14-xviii

Monitoring Air Time Fairness 14-xix
Monitoring ATF Statistics 14-xix

Monitoring Rogue Access Points 14-xx
Detecting Rogue Devices 14-xx
Classifying Rogue Access Points 14-xxi
Monitoring Rogue AP Alarms 14-xxiii
Viewing Rogue AP Alarm Details 14-xxiv
Viewing Rogue Client Details 14-xxiv
Viewing Rogue AP History Details 14-xxv
Monitoring Ad hoc Rogues 14-xxv
  Monitoring Ad hoc Rogue Alarms 14-xxvi
  Viewing Ad hoc Rogue Alarm Details 14-xxvi
  Searching Rogue Clients Using Advanced Search 14-xxvii
  Monitoring Rogue Access Point Location, Tagging, and Containment 14-xxvii
  Detecting Access Points 14-xxviii
  Monitoring Rogue Alarm Events 14-xxix
  Viewing Rogue AP Event Details 14-xxix
  Monitoring Ad hoc Rogue Events 14-xxix
  Viewing Ad hoc Rogue Event Details 14-xxx
  Troubleshooting Unjoined Access Points 14-xxx
Monitoring Spectrum Experts 14-xxxi
Monitoring WiFi TDOA Receivers 14-xxxi
  Searching WiFi TDOA Receivers 14-xxxi
Monitoring Media Streams 14-xxxi
  Viewing Media Stream Details 14-xxxi
Radio Resource Management 14-xxxi
  Viewing the RRM Dashboard 14-xxxi
Monitoring Access Point Alarms 14-xxxi
  Monitoring Air Quality Alarms 14-xxxi
  Monitoring CleanAir Security Alarms 14-xxxi
  Monitoring Cisco Adaptive wIPS Alarms 14-xxxi
  Monitoring Cisco Adaptive wIPS Alarm Details 14-xxxi
  Monitoring Failure Objects 14-xxxi
  Monitoring Events for Rogue Access Points 14-xxxi
  Monitoring Events for Ad hoc Rogues 14-xxxi
  Monitoring Cisco Adaptive wIPS Events 14-xxxi
  Monitoring CleanAir Air Quality Events 14-xxxi
  Monitoring Interferer Security Risk Events 14-xl
  Monitoring Health Monitor Events 14-xl

CHAPTER 15

Creating Monitoring Policies and Thresholds 15-i
  Default Monitoring Policies 15-ii
    Modifying Default Monitoring Policies 15-iv
  Creating New Monitoring Policies 15-v
CHAPTER 16

Monitoring Alarms 16-i

What Is an Event? 16-ii
  Recurring Alarms and Events 16-iii

What Is an Alarm? 16-iii
Defining Alarm Thresholds 16-iv
Where to Find Alarms 16-v
Display Options 16-vi
  Viewing Options for Alarms, Events, and Syslogs 16-vi
  Displaying Alarm Icons 16-vi
  Changing Alarm Display Behavior 16-vi
  Modifying Alarm Failure Source Pattern 16-vii
  Customizing the Alarm Summary 16-viii
Changing Alarm Status 16-viii
  When to Acknowledge Alarms 16-ix
  Including Acknowledged and Cleared Alarms in Searches 16-x
Changing Alarm and Event Options 16-x
Configuring Alarm Severity Levels 16-x
Customizing Alarms and Events For Traps 16-x
  Modifying a Customized Trap Event 16-xi
What is an Alarm Policy? 16-xi
  Customizing Interface Alarm Policy 16-xii
  Customizing Controller Alarm Policy 16-xiii
  Customizing Access Point Alarm Policy 16-xiv
  Customizing Layer2 Switch Alarm Policy 16-xvii
  Customizing Wired Infrastructure Alarm Policy 16-xviii
Viewing the Alarm Policy Summary 16-xix
Restoring Default Settings 16-xix
Getting Help for Alarms 16-xx
Viewing Syslogs 16-xx
CHAPTER  17

Monitoring Clients and Users  17-i
About Wired and Wireless Clients  17-ii
Client Dashlets on the General Dashboard  17-ii
Client Dashboard  17-iii
Monitoring Clients and Users  17-iii
  Filtering Clients and Users  17-iii
  Viewing Clients and Users  17-iv
When to Use the Client Troubleshooting Tool  17-vi
Launching the Client Troubleshooting Tool  17-vi
  About the Client Troubleshooting Page  17-vii
  How the Client Troubleshooting Tool Gives Advice  17-viii
Searching for Clients  17-xi
Analyzing Client Connection Logs  17-xi
Viewing Client Event History and Event Logs  17-xii
Checking Client ISE Authentication History and Identity Services  17-xii
Checking Client Clean Air Environment  17-xiii
Running Diagnostic Tests on Problem Clients  17-xiii
When to Run Diagnostic Tests on Problem Clients  17-xiii
Pinging Problem Clients with Text Messages  17-xiv
Viewing Real Time Troubleshooting (RTTS) Details  17-xiv
  Debug Commands for RTTS  17-xv
Tracking Clients  17-xvi
Tracking Multiple Clients  17-xvii
  Specifying Notification Settings  17-xvii
When to Assign a Username  17-xviii
Identifying Unknown Users  17-xix
Modifying the Clients and Users Page  17-xix
Enabling Automatic Client Troubleshooting  17-xx
When to Obtain Radio Measurements for a Client  17-xx
Obtaining Radio Measurements for a Client  17-xx
  Radio Measurement Results for a Client  17-xxi
CHAPTER 18

Performance Routing Version 3 Based Network Monitoring 18-i

Performance Routing 18-ii
Getting Access to PfR Monitoring for a User Group 18-ii
PfR Monitoring Page 18-iii
  Site to Site PfR Events Table 18-iv
  PfR Filter Panel 18-iv
  Service Provider View and DSCP View Charts 18-v
  Time Slider 18-vi
  Viewing Site to Site PfR Topology 18-vi
  Troubleshooting the Sankey diagram 18-vii
  Comparing WAN Interfaces 18-viii

CHAPTER 19

Monitoring Wireless Technologies 19-i

Monitoring Radio Resource Management 19-ii
  Channel Change Notifications 19-ii
  Transmission Power Change Notifications 19-iii
  RF Grouping Notifications 19-iii
  RRM Dashboard 19-iii
Monitoring Interferers 19-iv
  Configuring the Search Results Display 19-v
Contents

Monitoring RFID Tags 19-v
  Searching RFID Tags 19-vi
  Checking RFID Tag Search Results 19-vi
  Viewing Tag List 19-vi
Monitoring Media Streams 19-vi
Troubleshooting Unjoined Access Points 19-vii
Monitoring Chokepoints 19-viii
  Adding a Chokepoint to the Prime Infrastructure Database 19-viii
  Adding a Chokepoint to a Prime Infrastructure Map 19-ix
  Removing a Chokepoint from the Prime Infrastructure Database 19-x
  Removing a Chokepoint from a Prime Infrastructure Map 19-x
  Editing a Chokepoint 19-x
Monitoring WiFi TDOA Receivers 19-xi
  Enhancing Tag Location Reporting with WiFi TDOA Receivers 19-xi
  Adding WiFi TDOA Receivers to Prime Infrastructure and Maps 19-xi

CHAPTER 20
Using Monitoring Tools 20-i
  Monitoring Wireless Voice Audit 20-ii
  Monitoring Wireless Voice Diagnostics 20-ii
  Monitoring Wireless Configuration Audit 20-iii
  Monitoring Autonomous AP Migration Analysis 20-iii
  Monitoring Location Accuracy 20-iv
    Enabling the Location Accuracy Tool 20-iv
    Scheduling a Location Accuracy Test 20-v
    Running an On-Demand Location Accuracy Test 20-vi
  Monitoring Packet Capture 20-vii

CHAPTER 21
Viewing Performance Graphs 21-i
  Creating Performance Graphs 21-ii
    Viewing Multiple Metrics on a Single Performance Graph 21-ii
  Performance Graphs Options 21-iii
CHAPTER 22

Troubleshooting 22-i

Getting Help from Cisco 22-ii
  Launching the Cisco Support Community 22-ii
  Opening a Support Case 22-iii
Checking an End User's Network Session Status 22-iii
Troubleshooting Authentication and Authorization 22-iv
Troubleshooting Network Attachments 22-iv
Troubleshooting Network Attachment Devices 22-v
Troubleshooting Site Network Devices 22-v
Troubleshooting the User Application and Site Bandwidth Utilization 22-vi
Troubleshooting User Problems 22-vii
Troubleshooting the User's Experience 22-vii
Troubleshooting Voice/Video Delivery to a Branch Office 22-viii
Troubleshooting Unjoined Access Points 22.ix
Troubleshooting Wireless Performance Problems 22-x
Root Cause and Impact analysis of Physical and Virtual Data Center Components 22-x
  Troubleshooting UCS Hardware Problems 22-xi
  Viewing Bandwidth on Fabric Interconnect Ports 22-xii

CHAPTER 23

Monitoring Multiple Prime Infrastructure Instances 23-i

Viewing the Operations Center Dashboards 23-iii
Configuring Devices Using Operations Center 23-iii
  Viewing Configuration Templates Using Operations Center 23-iii
  Deploying Configuration Templates 23-iv
  Distributing Configuration Templates Across Managed Servers 23-iv
Monitoring Your Network Using Operations Center 23-v
  Monitoring Devices Using Operations Center 23-vi
Using Virtual Domains With Operations Center 23-vi
  Role Based Access Control Support in Operations Center 23-viii
Managing and Monitoring Prime Infrastructure Servers Using Operations Center 23-viii
  Viewing the Prime Infrastructure Server Status Summary in Operations Center 23-ix
  Viewing Prime Infrastructure Server Software Updates in Operations Center 23-x
  Viewing Prime Infrastructure Server Reachability History in Operations Center 23-x
  Viewing Alarms and Events Using Operations Center 23-xi
## Table of Contents

- Viewing Clients and Users Using Operations Center 23-xii
- Cross-Launching Prime Infrastructure Using Operations Center 23-xii
- Running Reports With Operations Center 23-xii
- Operations Center FAQs 23-xiii

### PART 1

**Configuring Devices**

**CHAPTER 25**

**Configuring Network Devices** 25-i

**CHAPTER 26**

**Using Templates to Configure Devices** 26-i

- Guidelines for Planning Your Network Design 26-ii
- Creating Feature-Level Configuration Templates 26-iii
- Features and Technologies Templates 26-iii
  - Creating Features and Technologies Templates 26-iv
  - Deployment Flow for Configuration Templates Using the Wizard 26-v
- CLI Templates 26-vi
  - Prerequisites for Creating CLI Templates 26-vi
  - Creating CLI Configuration Templates 26-vii
  - Creating CLI Configuration Templates from Copied Code 26-xii
  - Exporting a Template 26-xii
  - Importing a CLI Configuration Template 26-xiii
  - Exporting CLI Variables 26-xiii
  - Importing CLI Variables 26-xiii
  - Example: Updating Passwords Using a CLI Template 26-xiv
  - Deployment Flow for CLI Templates using the Wizard 26-xv
- Composite Templates 26-xvi
  - Creating Composite Templates 26-xvi
  - Deployment Flow for Composite Templates Using the Wizard 26-xvii
- Feature Templates 26-xviii
- My Tags 26-xix
  - Tagging a New Configuration Template 26-xix
  - Tagging an Existing Template 26-xix
  - Associating a Tag With Multiple Templates 26-xx
Contents

Controller Templates 26-xx
  Creating Controller Templates 26-xxi
Configuring Client Profiling 26-xxiii
Configuring Mobile Concierge (802.11u) 26-xxiv
Access Point Groups 26-xxv
  Creating WLAN AP Groups Templates 26-xxv
  Adding Access Point Groups 26-xxvi
  Deleting Access Point Groups 26-xxvii
  Creating Policy Configuration Templates 26-xxviii
  Adding FlexConnect Users to FlexConnect AP Groups Templates 26-xxviii
  Creating General AAA Security Controller Templates 26-xxviii
RADIUS Authentication Templates 26-xxix
Creating RADIUS Fallback Templates 26-xxix
Creating RADIUS TACACS Fallback Templates 26-xxix
Local EAP General Templates 26-xxx
Local Network Users Templates 26-xxxi
User Login Policies Templates 26-xxxi
MAC Filter Template 26-xxxi
Access Point or MSE Authorization Templates 26-xxxi
Manually Disabled Client Template 26-xxxi
Client Exclusion Policies Templates 26-xxxiv
Access Point Authentication and MFP Templates 26-xxxiv
Web Authentication Templates 26-xxxv
External Web Auth Server Templates 26-xxxvii
Security Password Policy Template 26-xxxix
Security - Access Control Templates 26-xxxix
Creating a FlexConnect Access Control List Template 26-xliv
Creating Security - CPU Access Control List Templates 26-xliv
Creating a CPU Access Control List (ACL) Template 26-xliv
Creating Security - Rogue Templates 26-xliv
  Rogue AP Rules 26-xliv
  Creating a Rogue AP Rule Groups Template 26-xlv
  Deploying a Rogue AP Rule Groups Template 26-xlvi
  Viewing Deployed Rogue AP Rules 26-xlvi
  SIP Snooping 26-xlvii
Creating Management Templates 26-xlvii
Creating LyncSDN Templates 26-l
Creating AVC Profiles Templates 26-lii
Creating NetFlow Templates 26-liii
Wireless Controller Summary Information 27-iii
Controller-Specific Commands 27-iv
Auditing Controllers 27-v
Updating Controller Credentials 27-vi
Updating Controller Credentials in Bulk 27-vii
Rebooting Controllers 27-vii
Downloading Software to Controllers 27-viii
Configuring IPaddr Upload Configuration/Logs from Controllers 27-ix
Downloading IDS Signatures to Controllers 27-ix
Downloading Customized WebAuthentication Bundles to Controllers 27-x
Downloading Vendor Device Certificates to Controllers 27-x
Downloading Vendor CA Certificates to Controllers 27-xi
Saving Controller Configurations to Flash 27-xii
Synchronizing Configurations from Controllers 27-xii
Managing Controller Templates 27-xii
Replacing Old Controller Models with New Models 27-xiv
Modifying Controller Properties 27-xiv
Configuring Controller System Parameters 27-xv
Uploading Configuration and Logs from Controllers 27-xix
Configuring Controller System Interfaces 27-xxi
Adding Interfaces to Controllers 27-xxi
Viewing or Modifying Controller Interface Details 27-xxii
Configuring Controller System Interface Groups 27-xxiii
NAC Integration 27-xxv
Guidelines for Using SNMP NAC 27-xxv
Guidelines for Using RADIUS NAC 27-xxvi
Configuring NAC Out-of-Band Integration (SNMP NAC): Workflow 27-xxvi
Wired Guest Access 27-xxviii
Creating an Ingress Interface 27-xxxii
Creating an Egress Interface 27-xxxii
Configuring Controller Network Routes 27-xxxii
Viewing Controller Spanning Tree Protocol Parameters 27-xxxiii
Configuring Controller Mobility Groups 27-xxxiv
Background Scanning on 1510s in Mesh Networks 27-xxxvii
Configuring Controller QoS Profiles 27-xxxix
Configuring Controller DHCP Scopes 27-xl
Viewing Controller User Roles 27-xli
Adding a New Local Net User Role to Controllers 27-xli
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a Global Access Point Password</td>
<td>27-xli</td>
</tr>
<tr>
<td>Configuring Global CDP</td>
<td>27-xlii</td>
</tr>
<tr>
<td>Configuring AP 802.1X Supplicant Credentials</td>
<td>27-xliii</td>
</tr>
<tr>
<td>Configuring Controller DHCP</td>
<td>27-xlili</td>
</tr>
<tr>
<td>Configuring Access Point Timer Settings</td>
<td>27-xliv</td>
</tr>
<tr>
<td>Configuring Controller WLANs</td>
<td>27-xlvi</td>
</tr>
<tr>
<td>Configuring Controller WLANs</td>
<td>27-xlvi</td>
</tr>
<tr>
<td>Viewing Controller WLAN Configurations</td>
<td>27-xlvii</td>
</tr>
<tr>
<td>Adding Policies to Controller WLANs</td>
<td>27-xlvii</td>
</tr>
<tr>
<td>Configuring Mobile Concierge (802.11u) on WLANs</td>
<td>27-xlviii</td>
</tr>
<tr>
<td>Adding WLANs to Controllers</td>
<td>27-li</td>
</tr>
<tr>
<td>Deleting Controller WLANs</td>
<td>27-li</td>
</tr>
<tr>
<td>Scheduling Status Changes for Multiple Controller WLANs</td>
<td>27-lii</td>
</tr>
<tr>
<td>Viewing WLAN Mobility Anchors</td>
<td>27-liii</td>
</tr>
<tr>
<td>Working with WLAN AP Groups</td>
<td>27-liv</td>
</tr>
<tr>
<td>Creating Controller WLAN AP Groups</td>
<td>27-liv</td>
</tr>
<tr>
<td>Deleting Controller WLAN AP Groups</td>
<td>27-liv</td>
</tr>
<tr>
<td>Auditing Controller WLAN AP Groups</td>
<td>27-liv</td>
</tr>
<tr>
<td>Configuring FlexConnect on APs</td>
<td>27-lvii</td>
</tr>
<tr>
<td>Supported Platforms for FlexConnect</td>
<td>27-lviii</td>
</tr>
<tr>
<td>FlexConnect Guidelines and Limitations</td>
<td>27-lviii</td>
</tr>
<tr>
<td>FlexConnect Authentication Process</td>
<td>27-lix</td>
</tr>
<tr>
<td>FlexConnect Operation Modes</td>
<td>27-lix</td>
</tr>
<tr>
<td>FlexConnect States</td>
<td>27-lx</td>
</tr>
<tr>
<td>Configuring FlexConnect: Workflow</td>
<td>27-lxi</td>
</tr>
<tr>
<td>FlexConnect AP Groups</td>
<td>27-lxvi</td>
</tr>
<tr>
<td>Viewing FlexConnect AP Groups</td>
<td>27-lxviii</td>
</tr>
<tr>
<td>Configuring FlexConnect AP Groups</td>
<td>27-lxix</td>
</tr>
<tr>
<td>Verifying APs in FlexConnect Groups</td>
<td>27-lxx</td>
</tr>
<tr>
<td>Auditing FlexConnect Groups</td>
<td>27-lxx</td>
</tr>
<tr>
<td>Default FlexConnect Group</td>
<td>27-lxx</td>
</tr>
<tr>
<td>Moving APs from Default FlexConnect AP Group to another FlexConnect Group</td>
<td>27-lxxi</td>
</tr>
<tr>
<td>Delete FlexConnect AP Group</td>
<td>27-lxxi</td>
</tr>
<tr>
<td>Configuring Controller Security Parameters</td>
<td>27-lxxii</td>
</tr>
<tr>
<td>Configuring Controllers AAA Security</td>
<td>27-lxxiii</td>
</tr>
<tr>
<td>Configuring Controller Web Auth Certificates</td>
<td>27-lxxvii</td>
</tr>
<tr>
<td>Configuring Controller User Login Policies</td>
<td>27-lxxviii</td>
</tr>
<tr>
<td>Managing Manually Disabled Clients</td>
<td>27-lxxviii</td>
</tr>
<tr>
<td>Configuring Controller Access Control Lists</td>
<td>27-lxxix</td>
</tr>
</tbody>
</table>
Configuring Cisco Adaptive wIPS Profiles 27-clxxx
Accessing wIPS Profiles 27-clxxxi
Adding wIPS Profiles 27-clxxxii
Editing wIPS Profiles 27-clxxxiv
Applying wIPS Profiles 27-clxxxiv
Deleting wIPS Profiles 27-clxxxiv
Associating SSID Groups With wIPS Profiles 27-clxxxiv
Managing MSE High Availability Using Prime Infrastructure 27-clxxxvi
MSE HA Automatic vs Manual Failover and Failback 27-clxxxvi
Pairing MSE HA Servers 27-clxxxvii
Viewing Configured Parameters for MSE HA Devices 27-clxxxviii
Viewing MSE High Availability Status 27-clxxxix
Triggering MSE HA Manual Failover or Failback 27-clxxxix
Enabling Automatic MSE HA Failover and Failback 27-cxc
Unpairing MSE HA Servers 27-cxci
Auto Provisioning for Controllers 27-cxci

CHAPTER 28

Creating Controller Configuration Groups 28-i
Adding Controller Configuration Groups 28-ii
Configuring Controller Configuration Groups 28-iii
Adding or Removing Controllers from a Configuration Group 28-iv
Adding or Removing Templates from the Configuration Group 28-iv
Applying or Scheduling Configuration Groups 28-v
Auditing Configuration Groups 28-vi
Rebooting Configuration Groups 28-vii
Viewing Configuration Group Reports 28-viii
Downloading Software to Configuration Groups 28-viii
Downloading IDS Signatures to Configuration Groups 28-ix
Downloading Customized WebAuth to Configuration Groups 28-x
About Mobility 28-x
Intra-Controller Roaming 28-x
Inter-Controller Roaming 28-xi
Inter-Subnet Roaming 28-xii
Symmetric Tunneling 28-xiii
About Mobility Groups 28-xiv
When to Include Controllers in a Mobility Group 28-xvi
Messaging Among Mobility Groups 28-xvi
Configuring Mobility Groups: Workflow 28-xvi
Before You Begin Configuring Mobility Groups 28-xvii
Adding Controllers to Mobility Groups 28-xvii
Adding Controllers to Mobility Groups Manually 28-xviii
Setting Mobility Scalability Parameters 28-xix
Mobility Anchors 28-xx
Adding Multiple Controllers And Setting DCA Channels 28-xx
Configuring Controller Mobility Groups: Workflow 28-xxi

CHAPTER 29

Configuring Wireless Technologies 29-i
Chokepoints 29-ii
  Adding Chokepoints 29-ii
  Removing Chokepoints 29-ii
  Adding Chokepoints to Maps 29-iii
  Removing Chokepoints from Maps 29-iv
  Editing Chokepoints 29-iv
Wi-Fi TDOA Receivers 29-iv
  Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting 29-v
  Adding Wi-Fi TDOA Receivers 29-v
  Adding Wi-Fi TDOA Receivers to Maps 29-vi
  Editing Wi-Fi TDOA Receivers 29-vii
  Removing Wi-Fi TDOA Receivers 29-vii
Access Point Radios 29-vii
  Adding Autonomous Access Points to Prime Infrastructure 29-vii
  Configuring Access Point Details 29-xiii
  Importing AP Configuration 29-xxi
  Exporting AP Configuration 29-xxiii
  Configuring Access Points 802.11n Antenna 29-xxiii
  Configuring CDP 29-xxxii
  Configuring Access Points XOR Antenna 29-xxxii
  Configuring Access Point Radios for Tracking Optimized Monitor Mode 29-xxxv
  Copying and Replacing Access Points 29-xxxvi
  Bulk Copy and Replacing the Access Points 29-xxxvi
  Removing Access Points 29-xxxvii
  Scheduling and Viewing Radio Status 29-xxxvii
  Viewing Audit Status (for Access Points) 29-xxxviii
  Filtering Alarms for Maintenance Mode Access Points 29-xxxix
Integrating APIC-EM with Prime Infrastructure 32-v
Plug and Play Profiles 32-vi
Creating Plug and Play Profiles for Routers and Switches 32-vii
Creating Plug and Play Profiles for Wireless AP 32-ix
Prerequisites for Connecting a Nexus Device in the Network 32-ix
Creating Plug and Play Profiles for Nexus Devices 32-x
Activating Device Profiles 32-xi
Creating New Plug and Play Profiles and Adding Device Profiles 32-xii
Adding Device Profiles to an Existing Plug and Play Profile 32-xii
Adding Device Profiles into Router and Switches Plug and Play Profiles 32-xii
Importing Device Profiles into Plug and Play Profiles 32-xiv
Adding Device Profiles into Wireless AP Plug and Play Profiles 32-xv
Adding Device Profiles into Nexus Plug and Play Profiles 32-xvi
Supported Devices and Software Images for Plug and Play 32-xvii
Prerequisites for Deploying Bootstrap Configuration into a Device 32-xviii
Bootstrap Configuration 32-xviii
Methods of Installing Bootstrap Configurations 32-xxi
Exporting the Bootstrap Configuration 32-xxii
Exporting the Bootstrap Configuration Using TFTP 32-xxii
Emailing the Bootstrap Configuration 32-xxiii
Emailing the PIN for the Bootstrap Configuration 32-xxiii
Using DHCP to Export Bootstrap Configurations 32-xxiv
Verifying Device Status 32-xxv
Integrating Map View 32-xxv
Deleting Plug and Play Profiles 32-xxvii

PART 1

Managing Device Inventory

CHAPTER 34

Viewing Devices 34-i
Viewing Network Devices 34-ii
Viewing Compute Devices 34-iv
Creating User Defined UCS Groups 34-vii
Creating User Defined Hosts and VMs 34-vii
CHAPTER 35

Updating Device Inventory 35-i
  Changing Discovery Settings 35-ii
  Scheduling Discovery Jobs 35-iii
  Monitoring the Discovery Process 35-iii
  Discovery Protocols and CSV File Formats 35-iii
  Updating Device Inventory Manually 35-iv
    Editing Device Inventory Manually 35-iv
  Importing Device Inventory 35-v
  Using Credential Profiles 35-v
    Adding Credential Profiles 35-v
    Editing Credential Profiles 35-vi
    Deleting Credential Profiles 35-vii
    Copying Credential Profiles 35-vii
    Viewing Devices Associated with a Credential Profile 35-vii
  Troubleshooting Unmanaged Devices 35-viii

CHAPTER 36

Managing and Monitoring Compute Resources 36-i
  Managing VMware Vcenter Server 36-ii
    Adding VMware Vcenter Servers 36-ii
    CSV File Requirements for Importing Vcenter 36-ii
  Monitoring Performance of Compute Resources 36-iii
    Setting Polling Interval for Monitoring Compute Resources 36-iii
    Monitoring Clusters 36-iv

CHAPTER 37

Maintaining Software Images 37-i
  Overview of Software Image Management 37-ii
  Software Image Management Processes and Supported Devices 37-ii
  Setting Image Management and Distribution Preferences 37-iv
  Configuring Software Image Management Server for Image Distribution 37-v
  Managing Software Images 37-vi
  Importing Software Images 37-vi
  Importing Software Images to the Virtual Image Repository 37-vii
  Changing Software Image Requirements 37-viii
Supported Devices and Image Family 37-viii
Distributing Software Images to Devices 37-x
Activating Software Images 37-xi
Supported Image Format for Stack Devices 37-xii
Viewing Recommended Software Images from Cisco.com 37-xii
Analyzing Software Image Upgrades 37-xiii

CHAPTER 38

Working with Device Configurations 38-i

Configuration Archives 38-ii
Changing Prime Infrastructure Device Configuration Settings 38-ii
Changing Prime Infrastructure Configuration Archive Collection Settings 38-iii
  Supported Syslog Formats for Configuration Archive Collection Settings 38-iii
Comparing Current and Previous Device Configurations 38-iv
Scheduling Configuration Archive Tasks 38-iv
Overview of Device Configurations 38-v
  Changing a Single Device Configuration 38-v
  Adding a Wireless LAN Controller 38-vi
  Changing Wireless LAN Controller Configuration Settings 38-vi
  Rebooting Controllers 38-vi
Configuration Rollbacks 38-vii
Rolling Back Device Configuration Versions 38-vii
Deleting Device Configurations 38-viii

CHAPTER 39

Grouping Devices, Ports and Data Center 39-i

Types of Groups 39-ii
Accessing Device/Location Groups through Virtual Domains 39-ii
Creating Device Groups 39-iii
  Searching Device Groups 39-iv
Using Location Groups 39-iv
Creating Location Groups 39-v
  Location Groups and Wireless Maps 39-vi
  Importing Location Groups Using CSV File 39-vi
  Exporting Location Groups as CSV File 39-vi
  Editing User Defined and Location Groups 39-vii
# Contents

- Changing the Topology Map Layout 41-xvii
- Saving the Topology Map Layout 41-xvii
- Saving the Topology Map as an Image File 41-xviii
- Creating a Topology Dashlet 41-xviii
- Viewing vPc Summary 41-xix

## CHAPTER 42

### Using Wireless Maps 42-i

- About Prime Infrastructure Site Maps 42-ii
  - Site Map Hierarchy 42-ii
  - Site Map Graphics 42-iii
  - Network Elements on Site Maps 42-iii
  - Wireless Coverage Areas, Inclusion/Exclusion Regions and Rail Lines on Maps 42-iii
- Preparing Image Files for Use with Prime Infrastructure Maps 42-iv
  - Troubleshooting Problems With CAD Image File Imports 42-iv
  - Default Campus Maps 42-v
  - Disabling Next Generation Maps 42-v
- Working With Site Maps 42-vi
- Creating Campus Maps 42-vi
- Adding Image Files to Campus Maps 42-vii
- Adding Location Information to Campus Maps 42-viii
- Changing Default Map Measurement Units 42-viii
- Adding Buildings to Campus Maps 42-ix
  - Moving Buildings and Floors to Another Campus 42-x
- Adding Floor Areas to Buildings 42-x
- Adding Image Files to Floor Areas 42-xii
  - Getting AP Details from 360° View 42-xv
- Monitoring Floor Areas 42-xxviii
  - Panning and Zooming with Next Generation Maps 42-xxviii
  - Floor View Navigation 42-xxix
  - Adding Access Points to a Floor Area 42-xxix
- Using the Automatic Hierarchy to Create Maps 42-xxxii
- Using the Map Editor 42-xxxv
  - Guidelines for Using the Map Editor 42-xxxv
  - Guidelines for Placing Access Points 42-xxxv
  - Guidelines for Inclusion and Exclusion Areas on a Floor 42-xxxvii
  - Opening the Map Editor 42-xxxviii
Map Editor Icons 42-xxxviii
Using the Map Editor to Draw Coverage Areas 42-xxxix
Using the Map Editor to Draw Obstacles 42-xl
Defining an Inclusion Region on a Floor 42-xl
Defining an Exclusion Region on a Floor 42-xl
Defining a Rail Line on a Floor 42-xl

Adding an Outdoor Area 42-xl

Using Chokepoints to Enhance Tag Location Reporting 42-xl
Adding Chokepoints to Prime Infrastructure 42-xl
Adding a Chokepoint to a Prime Infrastructure Map 42-xl
Positioning Chokepoints 42-xl

Configuring Wi-Fi TDOA Receivers 42-xl
Adding Wi-Fi TDOA Receivers to Prime Infrastructure 42-xl
Adding Wi-Fi TDOA Receivers to a Map 42-xl
Positioning Wi-Fi TDOA Receivers 42-xl
Managing RF Calibration Models 42-xl
Managing Location Presence Information 42-xl

Searching Maps 42-lxii

Using the Map Editor 42-lxii
Inspecting Location Readiness and Quality 42-lxiii
Inspecting Location Readiness 42-lxiii
Inspecting Location Quality Using Calibration Data 42-lxiii
Inspecting VoWLAN Readiness 42-lxiv
Troubleshooting Voice RF Coverage Issues 42-lxv

Monitoring Mesh Networks Using Maps 42-lxv
Monitoring Mesh Link Statistics Using Maps 42-lxv
Monitoring Mesh Access Points Using Maps 42-lxvii
Monitoring Mesh Access Point Neighbors Using Maps 42-lxviii
Viewing the Mesh Network Hierarchy 42-lxix
Using Mesh Filters to Modify Map Display of Maps and Mesh Links 42-lxx

Monitoring Tags Using Maps 42-lxxii

Using Planning Mode 42-lxxii
Accessing Planning Mode 42-lxxii
Using Planning Mode to Calculate Access Point Requirements 42-lxxiv
Wireless Map Refresh Options 42-lxxviii
Understanding RF Heatmap Calculation 42-lxxix
Drawing Polygon Areas in Wireless Maps 42-lxxix
Floor View in Wireless Maps 42-lxxx

Associating Endpoints with a Site 42-lxxxi
PART 1

Ensuring Network Services

CHAPTER 44

Securing Network Services 44-i

CHAPTER 45

Configuring and Monitoring IWAN 45-i
  Prerequisites for Enabling IWAN Services 45-ii
  Using the IWAN Wizard 45-iv
  Using PKI with IWAN-DMVPN Service 45-v

CHAPTER 46

Using Converged Access Workflow 46-i
  Converged Access Workflow Overview 46-ii
  Supported Cisco IOS-XE Platforms 46-iv
  Prerequisites for Converged Access Deployment 46-v
    Prerequisites for Layer 2 and Layer 3 46-v
    Prerequisites for Server Configuration 46-x
  Converged Access Template-Based Deployment 46-x
  Guidelines for Entering Configuration Values 46-xiii
    Converged Access Template Field Descriptions 46-xiii
    Entering Configuration Values for Controller-Less Single-Switch Deployment Model 46-xvii
    Entering Configuration Values for Controller-Less Single/Multi-Domain Wireless Deployment Model 46-xxiii
    Entering Configuration Values for Controller-Based Single/Multi-Domain Wireless Deployment Model 46-xxv
    Entering Configuration Values for Centralized Wireless Campus Deployment Model 46-xxvii

CHAPTER 47

Configuring Branch Threat Defense 47-i
  Supported IOS-XE Platforms 47-ii
  Supported IOS-XE Versions 47-ii
  Prerequisites for Enabling Branch Threat Defense 47-ii
  Using the Branch Threat Defense Wizard 47-iii
Enabling Data Deduplication 50-xiii

Creating a VPN Component Template 50-xiii
   Creating an IKE Policies Template 50-xiii
   Creating an IKE Settings Template 50-xiv
   Creating an IPsec Profile Template 50-xiv
   Creating a Preshared Keys Template 50-xv
   Creating RSA Keys Template 50-xv
   Creating a Transform Sets Template 50-xv

Configuring an Easy VPN Server 50-xvi
   Creating an Easy VPN Server Proxy Setting Template 50-xvi
   Creating an Easy VPN Remote Template 50-xvii
   Creating an Easy VPN Server Template 50-xviii
   Creating a GSM Profile Template 50-xix
   Creating a Cellular Profile Template 50-xix

Redirecting HTTP and HTTPS Traffic 50-xx

Configuring Interfaces 50-xxi
   Configuring a Serial Interface 50-xxi
   Configuring POS Interface 50-xxii
   Configuring a Service Module 50-xxii
   Configuring Controllers 50-xxiii
   Creating a Gigabit Ethernet or Fast Ethernet Interface 50-xxiii
   Creating a Loopback Interface 50-xxiv
   Creating a VLAN Interface 50-xxiv
   Editing a VLAN Interface 50-xxv
   Creating a Tunnel Interface 50-xxv
   Editing an Existing Tunnel Interface 50-xxv
   Creating a Virtual Template Interface 50-xxvi
   Editing an Existing Virtual Template Interface 50-xxvi

Configuring Cellular WAN Interfaces 50-xxvii
   Configuring a CDMA Interfaces 50-xxvii
   Configuring a GSM Interfaces 50-xxvii

Configuring Network Address Translation (NAT) 50-xxviii
   NAT Types 50-xxviii
   Configuring NAT for IP Address Conservation 50-xxix
   Creating NAT IP Pools 50-xxix
   Creating NAT44 Rules 50-xxx
   Configuring Interfaces 50-xxx
   Setting Up NAT MAX Translation 50-xxx

Configuring DMVPN 50-xxx
Creating a DMVPN Tunnel 50-xxxii
Configuring Hub and Spoke Topology 50-xxxiii
Configuring a DMVPN Fully Meshed Topology 50-xxxiii
Configuring a Cluster Topology 50-xxxiv
Editing a DMVPN 50-xxxv
Deleting a DMVPN 50-xxxv

Configuring GETVPN 50-xxxv
Creating a GETVPN Group Member 50-xxxvi
Creating a GETVPN Key Server 50-xxxvii
Editing a GETVPN Group Member or Key Server 50-xxxviii
Deleting a GETVPN Group Member or Key Server 50-xxxviii

Configuring VPN Components 50-xxxix
Configuring IKE Policies 50-xxxix
Configuring IKE Settings 50-xl
Configuring IPsec Profiles 50-xl
Creating Preshared Keys 50-xl
Creating RSA Keys 50-xli
Configuring Transform Sets 50-xlii

Creating a Zone-Based Firewall 50-xlili
Configuring a Zone-Based Firewall Template 50-xliv
Creating an Interface Role 50-xlv
Creating an IPv4 Network Object 50-xlv
Defining Device Override 50-xlv
Creating a Zone-Based Firewall Policy Rules Template 50-xlvi
Configuring a Zone-Based Firewall on a Single Device 50-xlvi

Creating a Routing Protocol 50-liii
Creating a Static Route 50-liii
Creating a RIP Route 50-liiv
Creating an EIGRP Route 50-lv
Creating an OSPF Route 50-lv
Configuring NAM with Application Servers 50-lvi

CHAPTER 51

Ensuring Consistent Application Experiences 51-i
Evaluating Service Health 51-iii
Creating Custom Applications 51-iv
Service Health Window 51-iv
Viewing the Health Timeline 51-v
Contents

Adding a Location Server 55-x

Synchronizing Prime Infrastructure and MSE 55-x
  Synchronizing Controllers with MSEs 55-xii
  Managing Third-Party Elements on MSEs 55-xiv
  Setting and Verifying the Controller Time Zones 55-xiv
  Configuring Smart Mobility Services Engine Database Synchronization 55-xv
  Viewing MSE Synchronization Status 55-xvii
  Viewing Synchronization History 55-xvii

Viewing MSE Notification Statistics 55-xviii

Editing MSE General Properties for MSE 55-xix
  Editing NMSP Parameters for MSE 55-xx
  Viewing Active Session Details for MSE 55-xxi
  Viewing Trap Destinations for MSE 55-xxii
  Adding Trap Destinations for MSE 55-xxii
  Editing Advanced Parameters for MSE 55-xxiii
  Rebooting the MSE Hardware 55-xxiv
  Shutting Down the MSE Hardware 55-xxiv
  Clearing the MSE Database 55-xxv
  Configuring MSE Logging Options 55-xxv

Adding MSE Users 55-xxvii
  Deleting MSE Users 55-xxvii
  Editing User Properties 55-xxvii

Adding User Groups 55-xxviii
  Deleting User Groups 55-xxviii
  Editing Group User Permissions 55-xxix

Monitoring Status Information for MSEs 55-xxix
  Viewing MSE Server Events 55-xxix
  Viewing MSE Audit Logs 55-xxx
  Viewing MSE Alarms 55-xxx
  Out-of-Sync Alarms 55-xxx
  Viewing MSE Events 55-xxx
  Viewing MSE NMSP Connection Status 55-xxx
  Editing MSE Backup Parameters 55-xxx
  Backing Up MSE Historical Data 55-xxx
  Restoring MSE Historical Data 55-xxx
  Downloading Software to MSEs 55-xxx
  Configuring Partner Systems for MSEs 55-xxx
  Managing Cisco Adaptive wIPS Service Parameters 55-xxx
  Managing Context-Aware Service Software Parameters 55-xxxvii
Contents

Context-Aware Service General Parameters  55-xxxviii
Modifying Tracking Parameters for Mobility Services  55-xxxviii
Filtering Parameters for Mobility Services  55-xli
Modifying History Parameters for Mobility Services  55-xlili
Enabling Location Presence for Mobility Services  55-xliv
Importing Asset Information for Mobility Services  55-xlv
Exporting Asset Information for Mobility Services  55-xlvi
Importing Civic Information for Mobility Services  55-xlvi
Context-Aware Service Wired Parameters  55-xlvii
Context-Aware Service Advanced Parameters  55-xlxi
Viewing MSE Notifications Summary  55-liv
Viewing and Managing MSE Notifications  55-lv
Viewing Notification Statistics  55-lvi
Mobile Concierge Service Parameters  55-lvii

Event Groups  55-lvii
Adding Event Groups  55-lvii
Deleting Event Groups  55-lviii
Working with Event Definitions  55-lviii
Adding Event Definitions  55-lx
Deleting an Event Definition  55-lxiii
Searching for Wireless Client on MSE by IPv6 Address  55-lxiv
Viewing Clients Detected by MSE  55-lxv
Viewing MSE Alarm Details  55-lxvii

Monitoring with Mobile Concierge Services  55-lxviii
Defining Venues  55-lxviii
Deleting Venues  55-lxix
Defining Providers with Policies  55-lxx
Deleting Providers  55-lxxi
Defining Policies  55-lxxi
Deleting Policies  55-lxxii

Configuring and Deploying wIPS Solution Using the Wireless Security Configuration Wizard  55-lxxiii

CHAPTER  56

Configuring the Cisco AppNav Solution  56-i
Overview of Cisco AppNav  56-ii
Components of Cisco AppNav  56-ii
Prerequisites for Configuring Cisco AppNav  56-iv
Configuring Cisco AppNav  56-iv
Chapter 57

Configuring the Cisco WAAS Container

Prerequisites for Installing an ISR-WAAS Container
Cisco WAAS Central Manager Integration
Cisco WAAS Central Manager Integration
Configuring Single Sign-On
Creating a Username in Cisco WAAS Central Manager
Cross-Launching Cisco WAAS Central Manager
Defining Interface Roles
Importing an OVA image
Configuring Cisco AppNav Automatically During ISR-WAAS Container Activation
Installing an ISR-WAAS Container
Installing and Activating an ISR-WAAS Container
Installing an ISR-WAAS Container on a Single Router
Installing an ISR-WAAS Container on Multiple Routers
Uninstalling and Deactivating a Cisco WAAS Container
Uninstalling a Single Cisco ISR-WAAS Container
Uninstalling a Multiple Cisco ISR-WAAS Container
Deactivating a Cisco ISR-WAAS Container

Chapter 58

Working with Wireless Mobility

What Is Mobility?
New Mobility
Mobility Work Center
Creating a Mobility Domain
Creating a Switch Peer Group
Changing a Mobility Role
Mobility Anchors
Configuring a Guest Anchor Controller for a WLAN
Configuring Spectrum Experts
Adding a Spectrum Expert
Getting Started

- Introduction to Cisco Prime Infrastructure
- Adding Licenses
- Adding Devices to Prime Infrastructure
- Grouping Devices
- Setting Up Network Monitoring
- Changing User Settings
Cisco Prime Infrastructure is a network management tool that supports lifecycle management of your entire network infrastructure from one graphical interface. Prime Infrastructure provides network administrators with a single solution for provisioning, monitoring, optimizing, and troubleshooting both wired and wireless devices. Robust graphical interfaces make device deployments and operations simple and cost-effective.

Prime Infrastructure Organization

The Prime Infrastructure web interface is organized into a lifecycle workflow that includes the high-level task areas described in Table 4-1. This document follows the same general organization.

<table>
<thead>
<tr>
<th>Task Area</th>
<th>Description</th>
<th>Used By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>View dashboards, which give you a quick view of devices, performance information, and various incidents. See Filters for more information.</td>
<td>Network Operators, and Network Engineers</td>
</tr>
<tr>
<td>Monitor</td>
<td>Monitor your network on a daily basis and perform other day-to-day or ad hoc operations related to network device inventory and configuration management. The Monitor tab includes dashboards and tools that you need for day-to-day monitoring, troubleshooting, maintenance, and operations.</td>
<td>Network Engineers, Designers, and Architects</td>
</tr>
<tr>
<td>Configuration</td>
<td>Design feature or device patterns, or templates. You create reusable design patterns, such as configuration templates, in the Design area. You may use predefined templates or create your own. Patterns and templates are used in the deployment phase of the lifecycle. You can also design Plug and Play profiles and mobility services.</td>
<td>Network Engineers, Designers, and Architects</td>
</tr>
</tbody>
</table>

Caution: You are strongly advised not to enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing Tools > Internet Options and unselecting the Enable third-party browser extensions check box in the Advanced tab.
### Table 4-1  Prime Infrastructure Task Areas  (continued)

<table>
<thead>
<tr>
<th>Task Area</th>
<th>Description</th>
<th>Used By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Perform all device management operations such as adding devices, running discovery, managing software images, configuring device archives, and auditing configuration changes on devices.</td>
<td>Network Engineers, NOC Operators and Service Operators</td>
</tr>
<tr>
<td>Maps</td>
<td>View network topology and wireless maps.</td>
<td>Network Engineers, NOC Operators, and Service Operators</td>
</tr>
<tr>
<td>Services</td>
<td>Access mobility services, Application Visibility and Control services, and IWAN features.</td>
<td>Network Engineers, NOC Operators and Service Operators</td>
</tr>
<tr>
<td>Report</td>
<td>Create reports, view saved report templates, and run scheduled reports.</td>
<td>Network Engineers, NOC Operators, and Service Operators</td>
</tr>
<tr>
<td>Administration</td>
<td>Specify system configuration settings and data collection settings, and manage access control. You can view and approve jobs, specify health rules, and manage licenses. You can also perform software updates and configure high availability.</td>
<td>Network Engineers</td>
</tr>
</tbody>
</table>

**Related Topic**
- [Understanding the Prime Infrastructure User Interface](#)
Adding Licenses

About Traditional Licenses

You must purchase licenses to access the Cisco Prime Infrastructure features required to manage your network. Each license also controls the number of devices that you can manage using those features. The maximum number of license files that can be added to Prime Infrastructure is 25.

You need a base license and the corresponding feature licenses (such as the assurance or the lifecycle license) to get full access to the respective Prime Infrastructure features to manage a set number of devices.

When you install Prime Infrastructure for the first time, you can access the lifecycle, assurance, collector, and data center features using the built-in evaluation license that is available by default. The default evaluation limitations are as follows:

- The Lifecycle and Assurance license is valid for 60 days for 100 devices.
- The Collector License is valid for 60 days for 20,000 Netflow per seconds.
- The Data Center License is valid for 60 days for 10 devices.

Data Center Hypervisor License was introduced in Prime Infrastructure version 3.0. This license is not available by default and is added explicitly to manage the V-center devices (hosts). The V-center devices are added in Inventory > Device Management > Compute Devices > Discovery Sources. The Data Center Hypervisor License added in Administration > Licenses and Software Updates > Licenses > Files > License Files automatically manages the number of hosts.

For information about Prime Infrastructure license types and how to order them, see the Cisco Prime Infrastructure 3.0 Ordering and Licensing Guide.

See the Cisco Prime Infrastructure 3.1 Administrator Guide for information about managing licenses, troubleshooting licensing issues, verifying license details and about the different types of licenses.

Adding a Traditional License to Access Features

You purchase licenses to access the Prime Infrastructure features required to manage your network. Each license also controls the number of devices or the number of devices on which NetFlow is enabled that you can manage using those features.

To add a new license, follow these steps:

**Step 1** Choose Administration > Licenses and Software Updates > Licenses.
Step 2  Click **Files**, then click **License Files**.

Step 3  Select the licenses that you have ordered with the required device limit, then click **Add**.

Step 4  Browse to the location of the license file, then click **OK**.

See the *Cisco Prime Infrastructure 3.1 Administrator Guide* for information about managing licenses, deleting licenses, troubleshooting licensing issues, and verifying license details.

### About the Smart License Feature

From Cisco Prime Infrastructure 3.1 version onwards, Smart Licensing feature is supported. This Smart Licensing feature provides a standardized licensing platform that simplifies user experience by reducing license-related complexity.

The benefits of this feature are:

- Licenses are not node-locked to devices which simplifies the Return-Merchandise-Authorization (RMA) process.
- Saves time with ability to transfer licenses across the company.
- Licenses can be pooled across the entire company, enabling them to be reused across organizational boundaries.
- Provides software asset management information so that you can plan and easily track if you have purchased adequate licenses.

For more details, please refer the Smart Licensing section of the *Cisco Prime Infrastructure 3.1 Administrator Guide* for enabling smart license, modifying the smart licensing transport details and performing other required actions on smart licenses.
Adding Devices to Prime Infrastructure

Methods for Adding Devices

You can add devices to Cisco Prime Infrastructure in one of the following ways:

- Use an automated process—See Adding Devices Using Discovery.
- Import devices from a CSV file—See Importing Devices from Another Source.
- Add devices manually by entering IP address and device credential information—See Adding Devices Manually.

Adding Devices Using Discovery

When you run discovery, Prime Infrastructure discovers the devices and, after obtaining access, collects device inventory data. We recommend that you run discovery, when you are initially getting started with Prime Infrastructure.

Prime Infrastructure uses SNMP polling to gather information about your network devices within the range of IP addresses you specify. If you have CDP enabled on your network devices, Prime Infrastructure uses the seed device you specify to discover the devices in your network.

You can discover your devices by:

- Configuring discovery settings—This method is recommended if you want to specify settings and rerun discovery in the future using the same settings. See Running Discovery.
- Running Quick Discovery—Quick Discovery quickly ping sweeps your network and uses SNMP polling to get details on the devices. See Running Quick Discovery.

Understanding the Discovery Process

Prime Infrastructure performs the following steps during the discovery process:

1. Using ICMP ping, determine if each device is reachable. If Prime Infrastructure is unable to reach the device, the device Reachability status is Unreachable.
2. Verify the SNMP credentials. If the device is reachable by ICMP, but the SNMP credentials are not valid, the device Reachability status is Ping Reachable.
   If the device is reachable by both ICMP and SNMP, the device Reachability status is Reachable.
3. Verify Telnet and SSH credentials.
4. Modify the device configuration(s) to add a trap receiver in order for Prime Infrastructure to receive the necessary notifications.
5. Start the inventory collection process to gather all device information.
6. Add the devices to the Inventory > Network Devices page.

Running Discovery

Prime Infrastructure discovers devices with IPv4 and IPv6 addresses. To run discovery, follow these steps:

Step 1  Choose Inventory > Device Management > Discovery.
Step 2  Click Discovery Settings (in the top right corner), then click New.
Step 3  Enter the Protocol Settings as described in Table 6-1.
Step 4  Perform one of the following:
   - Click Save to save your discovery settings and schedule your discovery to run at a specified time.
   - Click Run Now to run the discovery now.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Settings</td>
<td></td>
</tr>
<tr>
<td>Ping Sweep Module</td>
<td>Prime Infrastructure gets a list of IP address ranges from a specified combination of IP address and subnet mask, then pings each IP address in the range to check the reachability of devices. See Sample IPv4 IP Addresses for Ping Sweep for more information.</td>
</tr>
<tr>
<td>Layer 2 Protocols</td>
<td></td>
</tr>
</tbody>
</table>
| CDP Module           | Prime Infrastructure reads the cdpCacheAddress and cdpCacheAddressType MIB objects in the cdpCacheTable from CISCO-CDP-MIB on every newly found device as follows:
   1. The cdpCacheAddress MIB object is gathered from the current device. This provides a list of neighbor device addresses.
   2. If the neighbor device addresses do not already exist in the global device list, they are added to the local cache.
Select the Enable Cross Router Boundary check box to specify that Prime Infrastructure should discover neighboring routers. |
| LLDP                 | Similar to CDP, but it allows the discovery of non-Cisco devices. |
| Advanced Protocols   |             |
| Routing Table        | Queries and analyzes routing tables on seed routers to discover subnets and next-hop routers. This process discovers a router for every subnet on its list of known networks. |
### Address Resolution Protocol

The ARP Discovery Module depends on the Routing Table Discovery Module (RTDM), and is executed only when RTDM is processed. This precondition is identified based on the flags processed by the ARP Discovery Module, which are part of the DeviceObject.

The entries coming out of the ARP Discovery Module do not need to pass through RTDM because (per the router Discovery algorithm) active routers are those that RTDM must process and identify.

When the ARP table is fetched and the entries are not already discovered by RTDM, these entries (though they may represent routers) are not active routers and need not be passed on to RTDM. This is ensured by setting the ARP Discovery Module flag to Processed and leaving the RTDM flag set to Unprocessed.

When the RTDM comes across an entry with the RTDM flag unset and the ARP flag set, RTDM identifies the entry as an inactive router or other device and it leaves the entry as unprocessed. The ARP Discovery Module also ignores the entry according to the algorithm, based on the Processed flag set against the ARP Discovery Module.

When the **Enable ARP** check box is selected, the device MAC address needs to be updated in the device information. Applications can retrieve this information in the adapter through the DeviceInfo object. By scanning the device MAC address, the applications can distinguish between Cisco and non-Cisco devices.

ARP cache from the device is collected using CidsARPInfoCollector. The MAC ID of the device is retrieved from this data and set in the DeviceInfo object.

### Border Gateway Protocol

The BGP Discovery Module uses bgpPeerTable in the BGP4-MIB to find its BGP peer. The table contains its peers’ IP addresses, which are added as clues to the local cache.

### Open Shortest Path First

Open Shortest Path First (OSPF) protocol is an interior gateway routing protocol that uses the ospfNbrTable and ospfVirtNbrTable MIBs to find neighbor IP addresses.

### Filters

#### IP Filter

Includes or excludes devices based on IP address. For example, you can enter any of the following strings and specify whether to include or exclude the devices found during discovery:

- 192.0.2.89
- 192.0.2.*
- 192.0.[16-32].89
- [192-193].*.55.[16-32]

#### Advanced Filters

- **System Location Filter**
  Includes or excludes devices based on System Location.

- **System Object ID Filter**
  Includes or excludes devices based on the sysObjectID string set on the device.

- **DNS Filter**
  Includes or excludes devices based on the domain name string set on the device.

### Credential Settings

#### Credential Set

The credential set lists all the available credential profiles in Prime Infrastructure. You can associate credential profile with a range of IP addresses. The devices will be discovered based on the selected credential profile. For more information see, Using Credential Profiles.

#### SNMPv2 Credential

SNMP community string is a required parameter for discovering devices in the network using SNMPv2. You can enter multiple rows of credentials mapped to a specific IP address, or the IP address can be a wildcard; for example, *,.*,.*, 10.1.1.*. You cannot save or use the discovery settings if you do not specify SNMP credentials.
Adding Devices to Prime Infrastructure

Chapter 6

Adding Devices Using Discovery

After running discovery, choose Inventory > Device Management > Network Devices.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv3 Credential</td>
<td>Prime Infrastructure supports SNMPv3 discovery for devices. The following SNMPv3 modes are available:</td>
</tr>
<tr>
<td></td>
<td>- AuthPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) and AES-128 standards.</td>
</tr>
<tr>
<td></td>
<td>- AuthNoPriv—Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.</td>
</tr>
<tr>
<td></td>
<td>- NoAuthNoPriv—Uses a username match for authentication.</td>
</tr>
<tr>
<td></td>
<td>- PrivType—Protocol used to secure the SNMP authentication request.</td>
</tr>
<tr>
<td></td>
<td>- PrivPassword—Prefixed privacy passphrase for the SNMPv3 user.</td>
</tr>
<tr>
<td>Telnet Credential</td>
<td>You can specify the Telnet credentials during discovery so that Prime Infrastructure can collect the device configurations and fully manage the devices. If you do not specify Telnet credentials in the discovery settings, Prime Infrastructure discovers the devices but is unable to collect the full inventory of the device until you specify the Telnet credentials.</td>
</tr>
<tr>
<td>SSH Credential</td>
<td>For full device support via SSH, you must use SSHv2 with a 1024 bit key. You can configure SSH before running discovery. We recommend that you select SSHv2 as the protocol for communicating with the device CLI because it allows the use of Web Services Management Agent (WSMA) for configuring devices. (For more information see, Configuring the Device using WSMA.)</td>
</tr>
<tr>
<td>Preferred Management IP (how Prime Infrastructure attempts to find the preferred management address for devices)</td>
<td></td>
</tr>
<tr>
<td>Use Loopback IP</td>
<td>Prime Infrastructure uses the preferred management IP address from the loop back interface. If the device does not have a loopback interface, Prime Infrastructure uses similar logic to the OSPF algorithm to select the router’s preferred management IP address.</td>
</tr>
<tr>
<td>Use SysName</td>
<td>Prime Infrastructure gets the preferred management IP address for the device using DNS lookup of the SysName for the device.</td>
</tr>
<tr>
<td>Use DNS Reverse Lookup</td>
<td>Prime Infrastructure gets the preferred management IP address by doing a reverse DNS lookup on the device IP address, followed by a forward DNS lookup.</td>
</tr>
</tbody>
</table>

Table 6-1 Discovery Protocol Settings (continued)

After running discovery, choose Inventory > Device Management > Network Devices.

When discovery job redisCOVERs an existing device, the original credentials will be maintained and will not be updated with the credentials entered in Discovery Settings, if Last Inventory Collection Status of the device is “completed” in the Inventory > Device Management > Network Devices page. However, if the status is “partial collection” or any other status, then original credentials of the existing device will be overwritten with the credentials present in the Discovery Settings.

See Monitoring Network Devices for more information.
Sample IPv4 IP Addresses for Ping Sweep

### Table 6-2 Sample IPv4 Seed IP Addresses for Ping Sweep

<table>
<thead>
<tr>
<th>Subnet Range</th>
<th>Number of Bits</th>
<th>Number of IP Addresses</th>
<th>Sample Seed IP Address</th>
<th>Start IP Address</th>
<th>End IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>255.255.240.0</td>
<td>20</td>
<td>4094</td>
<td>10.104.62.11</td>
<td>10.104.48.1</td>
<td>10.104.63.254</td>
</tr>
<tr>
<td>255.255.248.0</td>
<td>21</td>
<td>2046</td>
<td>10.104.62.11</td>
<td>10.104.56.1</td>
<td>10.104.63.254</td>
</tr>
<tr>
<td>255.255.252.0</td>
<td>22</td>
<td>1022</td>
<td>10.104.62.11</td>
<td>10.104.60.1</td>
<td>10.104.63.254</td>
</tr>
<tr>
<td>255.255.254.0</td>
<td>23</td>
<td>510</td>
<td>10.104.62.11</td>
<td>10.104.62.1</td>
<td>10.104.63.254</td>
</tr>
<tr>
<td>255.255.255.0</td>
<td>24</td>
<td>254</td>
<td>10.104.62.11</td>
<td>10.104.62.1</td>
<td>10.104.62.254</td>
</tr>
<tr>
<td>255.255.255.128</td>
<td>25</td>
<td>126</td>
<td>10.104.62.11</td>
<td>10.104.62.1</td>
<td>10.104.62.126</td>
</tr>
<tr>
<td>255.255.255.192</td>
<td>26</td>
<td>62</td>
<td>10.104.62.11</td>
<td>10.104.62.1</td>
<td>10.104.62.62</td>
</tr>
<tr>
<td>255.255.255.224</td>
<td>27</td>
<td>30</td>
<td>10.104.62.11</td>
<td>10.104.62.1</td>
<td>10.104.62.30</td>
</tr>
<tr>
<td>255.255.255.248</td>
<td>29</td>
<td>6</td>
<td>10.104.62.11</td>
<td>10.104.62.9</td>
<td>10.104.62.14</td>
</tr>
<tr>
<td>255.255.255.252</td>
<td>30</td>
<td>2</td>
<td>10.104.62.11</td>
<td>10.104.62.9</td>
<td>10.104.62.10</td>
</tr>
<tr>
<td>255.255.255.254</td>
<td>31</td>
<td>0</td>
<td>10.104.62.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>32</td>
<td>1</td>
<td>10.104.62.11</td>
<td>10.104.62.11</td>
<td>10.104.62.11</td>
</tr>
</tbody>
</table>

### Running Quick Discovery

If you want to quickly run discovery without specifying and saving your settings, you can use Quick Discovery.

You can view the guest users discovered by Prime Infrastructure by choosing Services > Network Services > Guest Users. To see the correct lifetime on guest user accounts after they are discovered, make sure the devices have the correct time settings specified.

To run Quick Discovery, follow these steps:

**Step 1** Choose Inventory > Device Management > Discovery.

**Step 2** In the top-right side of the page, click Quick Discovery.

**Step 3** Complete the required fields, then click Run Now.

### Verifying Discovery

When discovery is completed, you can verify that the process was successful.

To verify successful discovery, follow these steps:

**Step 1** Choose Inventory > Device Management > Discovery.

**Step 2** Choose the discovery job for which you want to view details.
Chapter 6      Adding Devices to Prime Infrastructure

Importing Devices from Another Source

If you have another management system from which you want to import your devices, or if you want to import a spreadsheet that lists all of your devices and their attributes, you can add device information into Prime Infrastructure as explained in the following steps:

**Step 1** Choose **Inventory > Device Management > Network Devices**, then click **Bulk Import**.

**Step 2** From the **Operation** drop-down list, choose **Device**.

**Step 3** In the **Select CSV File**, enter or browse to the CSV file that contains the devices that you want to import.

**Step 4** Click the link to download a sample file that contains all of the fields and descriptions for the information that must be contained in your imported file. See **Figure 6-1**.

**Figure 6-1** Downloading a Sample Template for Importing Devices or Sites

![Bulk Import Interface](image)

Make sure that you retain the required information in the CSV file as explained in **CSV File Requirements for Importing Devices**.

If the importing CSV file contains any UDF parameters, ensure that UDF is configured in **Administration > Settings > System Settings > Inventory > User Defined Fields** prior to importing the devices. The UDF column in the CSV file must be begin with **UDF**: as indicated in the sample CSV template.

**Step 5** Click **Import**.
Step 6  Check the status of the import by choosing Administration > Dashboards > Job Dashboard > User Jobs > Import.

Step 7  Click the arrow to expand the job details and view the details and history for the import job.

CSV File Requirements for Importing Devices

If you want to use a CSV file to import your devices or sites from another source into Prime Infrastructure, you can download a sample template by choosing Inventory > Device Management > Network Devices, then clicking Bulk Import. Click the link to download a sample template as shown in Figure 6-1.

When you download a sample CSV template for importing devices or sites, the extent to which Prime Infrastructure can manage your devices, depends on the information you provide in the CSV file. If you do not provide values for CLI username, password, and enable password, Prime Infrastructure will have limited functionality and cannot modify device configurations, update device software images, and perform any other valuable functions. You can specify the credential profile in the CSV file to apply the credentials to a set of devices. If you specify the credential profile and also enter the values manually in the CSV file, then the manually entered credentials take high priority and the device is managed based on the combination of manually entered credentials and credential profile. For example, if the CSV file contains credential profile with SNMP and Telnet credentials in addition to manually entered SNMP credentials, then the device is managed based on the manually entered SNMP credentials and the Telnet credentials in the credential profile.

- For partial inventory collection in Prime Infrastructure, you must provide the following values in the CSV file:
  - Device IP address
  - SNMP version
  - SNMP read-only community strings
  - SNMP write community strings
  - SNMP retry value
  - SNMP timeout value

- For full inventory collection in Prime Infrastructure, you must provide the following values in the CSV file:
  - Device IP address
  - SNMP version
  - SNMP read-only community strings
  - SNMP write community strings
  - SNMP retry value
  - SNMP timeout value
  - Protocol

You must also provide values for the fields that correspond to the protocol you specify. For example, if you specify SNMPv3, you must specify values for the SNMPv3 fields in the sample CSV file such as the SNMPv3 username and authorization password.

- CLI username
Adding Devices Manually

Adding devices manually is helpful if you want to add a single device. If you want to add all devices in your network, we recommend that you run discovery (see Running Discovery) or import devices from a CSV file (see Importing Devices from Another Source).

After adding a device in the Converged view with profile, if you edit the device (which is associated with Credential Profile) in the Classic view, the Credential Profile association of the device is removed.

To add devices manually, follow these steps:

**Step 1** Choose **Inventory > Device Management > Network Devices**.

**Step 2** Click **Add Device**.

**Step 3** Complete the required fields.

**Step 4** For the License Level field, select

- **Full** to collect all device information and have Prime Infrastructure manage the device. Managed devices count against the number of managed devices in your Prime Infrastructure license. **Full** is selected by default.

- **Switch Port Trace Only** to collect partial device information (host name, device name, device type, and reachability status) and allow Prime Infrastructure to display how an AP is connected to a WLC on wireless maps. Switch Port Trace Only devices do not count against the number of managed devices in your Prime Infrastructure license. You cannot perform device management operations on devices that you designate as Switch Port Trace Only.

**Step 5** (Optional) Click **Verify Credentials** to verify the device credentials before adding the device.

**Note** Prime Infrastructure provides HTTP credentials verification support for NAM devices only.

**Step 6** Click **Add** to add the device with the settings you specified.

**Note** User Defined Field (UDF) parameters are available only if you added them under **Administration > Settings > System Settings > Inventory > User Defined Fields**. Do not use the special characters : ; and # for UDF field parameters.

Adding Virtual Device Context (VDC) Device

In Prime Infrastructure, Cisco NX-OS software supports Virtual Device Contexts (VDCs), which partition a single physical device into multiple logical devices that provide fault isolation, management isolation, address allocation isolation, service differentiation domains, and adaptive resource management. VDC allows the switches to be virtualized at the device level. It runs as a separate logical
entity within the switch, maintaining its own set of running software processes, having its own configuration, and being managed by an administrator. VDC1 is the default VDC (Admin VDC), and has a special role. You can configure child VDCs and allocate resources through default VDC.

Prime Infrastructure manages all Nexus features including VDC on Nexus devices running Cisco NX-OS software release 6.2(12) or later.

To add default VDC manually, follow these steps:

**Step 1** Choose **Inventory > Device Management > Network Devices**.
**Step 2** Click **Add Device**.
**Step 3** Complete the required fields.
**Step 4** (Optional) Click **Verify Credentials** to verify the device credentials before adding the device.
**Step 5** Click **Add** to add the device with the settings you specified.

After successful inventory collection, the device with Default VDC is added and subsequently child VDCs will be added automatically and the configuration will be stored in Prime Infrastructure database.

**About Adding Wireless Devices**

Note the following information when adding wireless devices to Prime Infrastructure:

- When a controller is removed from the system, a warning message appears to confirm whether the associated access points need to be removed.
- If you are adding a controller into the Prime Infrastructure across a GRE link using IPSec or a lower MTU link with multiple fragments, you might need to adjust the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU. If it is set too high, the controller might not be added into Prime Infrastructure.
- To adjust the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU: Stop the Prime Infrastructure, choose **Administration > Settings > System Settings > Network and Device > SNMP**, and edit the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU values to 50 or lower.
- When a controller is added to Prime Infrastructure, Prime Infrastructure acts as a TRAP receiver and the following traps are enabled on the controller: 802.11 Disassociation, 802.11 Deauthentication, and 802.11Authenticated.
- In the **Inventory > Network Devices > All Devices > Wireless Controllers** page, to update the credentials of multiple controllers in bulk, select the controllers you need to update and click **Edit**. Select the credential profile and click **Update** or **Update & Sync**.
- You can also update the credentials of multiple controllers in bulk by choosing a CSV file. Select the controllers and click **Bulk Import**. Browse the CSV file that contains a list of controllers to be updated, one controller per line. Each line is a comma separated list of controller attributes.
Validating That Devices Were Added Successfully

When a controller is added, the **Reachability** of the controller will be **Unknown**, while Prime Infrastructure attempts to communicate with the controller that you added. The Reachability of the controller changes to **Reachable** or **Ping Reachable** once the communication with the controller is successful.

When Compliance is enabled, the WLC can go to partial inventory collection state due to the following reasons:
- CLI credential does not have read-write privilege.
- WLC closes the connection during synchronization.
- WLC does not respond in the configured time out period.

Validating That Devices Were Added Successfully

After collecting device information, Prime Infrastructure gathers and displays the configurations and the software images for the devices. To verify that your devices were successfully added to Prime Infrastructure, you can choose **Inventory > Device Management > Network Devices** and

- Verify that the devices you have added appear in the list. Click a device name to view the device configurations and the software images that Prime Infrastructure collected from the devices.
- View details about the information that was collected from the device by hovering your mouse over the **Inventory Collection Status** field and clicking the icon that appears.
- Check the **Device Reachability Status** column. See Table 6-3 for status descriptions. HTTP/HTTPS parameters are verified on NAM devices only.
- Check the Admin Status column. See Table 6-4 for descriptions of the possible Admin Status values.
- To view details about the collection job and the details and history for the import job, choose **Administration > Dashboards > Job Dashboard**.

See Troubleshooting Unmanaged Devices for information about how to resolve any errors.

<table>
<thead>
<tr>
<th>Reachability Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Prime Infrastructure is able to reach the device using SNMP.</td>
</tr>
<tr>
<td>Yellow</td>
<td>The device is reachable using Ping, but not via SNMP. Verify that you specified the correct SNMP parameters for read access when the device was added to Prime Infrastructure.</td>
</tr>
<tr>
<td>Red</td>
<td>Prime Infrastructure is unable to reach the device using Ping. Verify that the device is operational and connected to the network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admin Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed</td>
<td>The device has been added successfully to Prime Infrastructure using SNMP.</td>
</tr>
</tbody>
</table>
Validating That Devices Were Added Successfully

Verifying Device Credentials

Prime Infrastructure automatically verifies device credentials as part of the inventory process. You can view device credential verification information by choosing Reports > Report Launch Pad > Device > Device Credential Verification.

Editing Device Parameters

You can edit the device parameters of a single device or multiple devices by choosing Inventory > Device Management > Network Devices.

To edit device parameters, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Inventory &gt; Device Management &gt; Network Devices.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select a single device or multiple devices and Click Edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Update the required parameters.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Update to update the parameters of all of the selected devices or Update &amp; Sync to update and synchronize the devices with the updated parameters.</td>
</tr>
</tbody>
</table>

Synchronizing Devices

To synchronize the Prime Infrastructure database with the configuration running on a device, you can force an inventory collection.

To synchronize devices, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Inventory &gt; Device Management &gt; Network Devices.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the device whose configuration you want synchronized with the configuration stored in the Prime Infrastructure database.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Sync.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admin Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unmanaged</td>
<td>The device credentials are incorrect or you have exceeded the number of devices allowed by your license. Choose Administration &gt; Licenses to view the status of your license. See the Cisco Prime Infrastructure 3.1 Administrator Guide for information about managing licenses, troubleshooting licensing issues, and verifying license details.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>You can manually change the Admin status of the added device to “Maintenance” from network device page. This will turn off processing and reception of any alarms and events from that device, and exclude the device from background synchronization jobs. You can change the Admin Status back to “Managed”, to enable the Alarms and background synchronization jobs.</td>
</tr>
</tbody>
</table>

Note: Table 6-4 Descriptions of Device Admin Status

Table 6-4 Descriptions of Device Admin Status

<table>
<thead>
<tr>
<th>Admin Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unmanaged</td>
<td>The device credentials are incorrect or you have exceeded the number of devices allowed by your license. Choose Administration &gt; Licenses to view the status of your license. See the Cisco Prime Infrastructure 3.1 Administrator Guide for information about managing licenses, troubleshooting licensing issues, and verifying license details.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>You can manually change the Admin status of the added device to “Maintenance” from network device page. This will turn off processing and reception of any alarms and events from that device, and exclude the device from background synchronization jobs. You can change the Admin Status back to “Managed”, to enable the Alarms and background synchronization jobs.</td>
</tr>
</tbody>
</table>
Adding NAM HTTP/HTTPS Credentials

If you are using Cisco Network Analysis Modules (NAMs) to monitor your network, you must add HTTPS credentials so that Prime Infrastructure can retrieve data from them. This is especially important for users who have licensed Assurance features, as most Assurance features depend on NAM data to work.

Prime Infrastructure polls NAMs directly via HTTP (or HTTPS) to collect their data. This type of polling requires Prime Infrastructure to store each NAMs’ HTTP credentials. Unlike with SNMP community strings and Telnet/SSH credentials, you cannot enter NAM HTTP credentials during the discovery process. You can only specify NAM HTTP credentials after the modules are discovered or added to inventory.

Follow these steps to add HTTP credentials for a single NAM. You can repeat this task for all NAMs from which you want Prime Infrastructure to collect data.

**Step 1** Choose Inventory > Device Management > Network Devices > Device Type > Cisco Interfaces and Modules > Network Analysis Modules.

**Step 2** Select one of the NAMs and click Edit.

**Step 3** In the Edit Device window, under Http Parameters:

- **Protocol**—Select the HTTP protocol, HTTP or HTTPS. The TCP Port will change automatically to the default port for the protocol that you have selected.
- **TCP Port**—Enter a different TCP Port if you want to override the default.
- **Username**—Enter the name of a user who can access the NAM via HTTP or HTTPS.
- **Password**—Enter the password for the username that you entered.
- **Confirm Password**—Re-enter the password to confirm.

**Step 4** Choose Update.

**Related Topics**

- Enabling NAM Data Collection
- Defining NAM Polling Parameters

Exporting Devices

In Prime Infrastructure, you can export device information as a CSV file. Prime Infrastructure does not export credential profiles.
To export devices, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Inventory &gt; Device Management &gt; Network Devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the devices that you want to export, then click Export Device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter an encryption password that will be used to open the exported CSV file.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Confirm the encryption Password and click Export to export the device information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Double-click the ExportDevice.zip file and enter the encryption password to open the ExportDevice.csv file.</td>
</tr>
</tbody>
</table>

⚠️ **Caution**  
The device export CSV file includes all device credentials and should be handled with appropriate care. Similarly, the privilege to allow device export should be assigned to appropriate users only.

**Next Steps**

Now that you have added devices to Prime Infrastructure, you can create device groups and port groups to simplify management, monitoring, and configuration of similar devices and ports. See Grouping Devices.

You might also want to:

- Plan for devices that will be added to your network in the future—See Preconfiguring Devices to be Added Later.
Grouping Devices

After you add devices to Prime Infrastructure, you can organize the devices into logical groupings to simplify management, monitoring, and configuration. When you group devices, you can perform operations on the entire group instead of selecting individual devices.

Grouping Devices by Device Type

You can group similar devices together to simplify management and configuration tasks. Depending on your needs, device groups can be based on location, device type, device role, and so on.

To create a device group, follow these steps:

**Step 1** Choose **Inventory > Device Management > Network Devices** or **Inventory > Group Management > Network Device Groups**.

**Step 2** In the **Device Groups** pane on the left, perform one of the following tasks:
- Click the expand icon next to **User Defined** and click **Add SubGroup**.
- Click the add icon and choose **Create User Defined Group** from the drop-down list.

**Step 3** Enter the name, description, and parent group if applicable.

**Step 4** Select one of the following for the new device group:
- **Add Device Manually**—You add devices to the group based on your needs.
- **Add Device Dynamically**—You specify the rules to which devices must comply before they are added to this device group. You do not add devices to dynamic groups. Prime Infrastructure adds devices that match the specified rules to the dynamic group.

**Step 5** Click **Preview** tab to view the devices that are automatically added to the group based on the specified rule and the manually added devices.

**Step 6** Click **Save**.

The device group that you created appears under the User Defined folder.

Related Topic
- Grouping Devices, Ports and Data Center
Setting Up Network Monitoring

After you add devices to the Prime Infrastructure inventory and set up device and port groups, you create monitoring templates to monitor device health (for example, CPU, memory, and interface utilization), basic QoS, and VPN tunnel statistics for wired devices in the group. After you create and apply monitoring templates, Prime Infrastructure collects and processes data from specified devices and displays the information in dashboards, dashlets, and reports.

- Monitoring Port Groups and Interfaces
- Getting Enhanced Client Information by Integrating with Cisco Identity Services Engine (ISE)
- Setting Up Assurance for Performance Monitoring

Monitoring Port Groups and Interfaces

To monitor your device ports, you can create a port group and then display monitoring information on Prime Infrastructure dashboards. Port groups are logical groupings of interfaces that allow you to monitor device ports by the function they serve. For example, you can create a port group for the WAN ports and create another port group for the internal distribution ports on the same router.

See Types of Groups and Creating Device Context or Group Context Port Groups for more information about creating port groups.

After you create groups, you can create an interface health monitoring policy on those ports as explained in the following steps:

Step 1  Choose Monitor > Monitoring Tools > Monitoring Policies.
Step 2  Click My Policies.
Step 3  Click Add.
Step 4  Choose Interface Health. under Policy Types.
Step 5  From the Device Selection drop-down list, choose Port Group.
Step 6  Choose the User Defined group and click OK.
Step 7  Enter the policy name.
Step 8  Select required the Parameters and Threshold and complete the required fields.
Step 9  Click OK.
Step 10 Click Save and Activate.
Step 11 To display the results, choose Dashboards > Overview > Network Interface, and view the Top N Interface Utilization dashlet.

Step 12 Edit the Top N Interface Utilization dashlet and add the port group that you previously created.

Related Topics
- Setting Up WAN Interface Monitoring
- Types of Groups
- Creating Device Context or Group Context Port Groups

Setting Up WAN Interface Monitoring

Creating a WAN interface port group allows you to efficiently monitor all WAN interfaces in a specific port group. For example, if you have many small branch offices that have low bandwidth issues, you can create a port group that includes all WAN interfaces from each branch office, and then monitor this port group for issues.

By default, Prime Infrastructure provides a static WAN Interfaces port group on which health monitoring is automatically deployed. The following procedure shows you how to:

1. Add interfaces to the WAN Interfaces port group.
2. Verify the utilization and availability of the WAN interfaces from the Site dashboard.

Step 1 To add interfaces to the WAN Interfaces port group:
   a. Choose Inventory > Group Management > Port Groups.
   b. From the menu on the left, choose System Defined > WAN Interfaces.
   c. Select the device, then click Add to Group.

Step 2 To display the results:
   a. Choose Dashboard> Overview > > Add Dashlets.
   b. Click either of the following:
      - Top N WAN Interfaces by Utilization
      - Top N WAN Interfaces with Issues

Getting Enhanced Client Information by Integrating with Cisco Identity Services Engine (ISE)

Prime Infrastructure manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, Prime Infrastructure collects additional information about these clients from Cisco ISE and provides all client relevant information to Prime Infrastructure to be visible in a single console.
When posture profiling is enforced in the network, Prime Infrastructure communicates with Cisco ISE to get the posture data for the clients and displays it along with other client attributes. When Cisco ISE is used to profile the clients or an endpoint in the network, Prime Infrastructure collects the profiled data to determine what type of client it is, whether it is an iPhone, iPad, an Android device, or any other device.

You can get enhanced information about managed clients using the Cisco ISE server.

If Prime Infrastructure is integrated with an ISE server (to access endpoint information), you can:

- Check an End User’s Network Session Status.
- Using the User 360° View, you can identify possible problems with the end user’s authentication and authorization for network access.
- Troubleshoot the User Application and Site Bandwidth Utilization.

Prime Infrastructure displays ISE Profiling attributes only for authenticated endpoints.

**Related Topics**
- Adding an Identity Services Engine

### Adding an Identity Services Engine

A maximum of two ISEs can be added to Prime Infrastructure. If you add two ISEs, one should be primary and the other should be standby. When you are adding a standalone node, you can add only one standalone node and cannot add a second node.

To add an Identity Services Engine, follow these steps:

1. **Step 1** Choose Administration > Servers > ISE Servers.
2. **Step 2** From the Select a command drop-down list, choose Add ISE Server, then click Go.
3. **Step 3** Complete the required fields, then click Save.

The credentials should be superuser credentials local to ISE. Otherwise, ISE integration does not work.

### Setting Up Assurance for Performance Monitoring

If your Prime Infrastructure implementation includes Assurance licenses, you must enable data collection via NAMs and NetFlow configurations. This is necessary to populate the additional dashlets, reports, and other features supplied with Assurance.

**Related Topics**
- Enabling NAM Data Collection
- Defining NAM Polling Parameters
- Enabling NetFlow Data Collection
Enabling NAM Data Collection

To ensure that you can collect data from your Network Analysis Modules (NAMs), you must enable NAM data collection. You can do this for each discovered or added NAM, or for all NAMs at the same time.

**Before You Begin**
You must specify the HTTP/HTTPS credentials for each NAM (see Adding NAM HTTP/HTTPS Credentials).

**Step 1** Choose Services > Application Visibility & Control > Data Sources.
**Step 2** In the NAM Data Collector section, select the required NAM datasources for which you want to enable data collection.
**Step 3** Click Enable.

Related Topics
- Defining NAM Polling Parameters
- Enabling NetFlow Data Collection

Defining NAM Polling Parameters

You can specify data that is collected from NAMs.

**Step 1** Choose Monitor > Monitoring Policies.
**Step 2** Click Add, then select NAM Health under the Policy Types list from the left sidebar menu.
**Step 3** Select the NAM devices from which you want to collect data, then complete the required fields.
**Step 4** Under Parameters and Thresholds, specify the parameters you want to poll from the NAM devices and threshold conditions.
**Step 5** Click Save and Activate.

Related Topics
- Enabling NetFlow Data Collection
- Enabling NAM Data Collection

Enabling NetFlow Data Collection

To start collecting NetFlow and Flexible NetFlow data, you must configure your NetFlow-enabled switches, routers, and other devices (ISR/ASR) to export this data to Prime Infrastructure. The following table shows the various device types that support NetFlow and the ways to configure devices to export NetFlow data to Prime Infrastructure.

Table 8-1 gives the detailed information of NetFlow support summary.
### Table 8-1 NetFlow Support Summary

<table>
<thead>
<tr>
<th>Device Type</th>
<th>IOS Versions Supporting NetFlow</th>
<th>Supported NetFlow Export Types</th>
<th>NetFlow Configuration in Prime Infrastructure</th>
<th>Template Naming Convention</th>
</tr>
</thead>
</table>
### Table 8-1  NetFlow Support Summary (continued)

<table>
<thead>
<tr>
<th>Device Type</th>
<th>IOS Versions Supporting NetFlow</th>
<th>Supported NetFlow Export Types</th>
<th>NetFlow Configuration in Prime Infrastructure</th>
<th>Template Naming Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISR</td>
<td>15.1(3) T</td>
<td>TCP/UDP conversation traffic Voice &amp; Video</td>
<td>TCP/UDP: Choose Configuration &gt; Templates &gt; Features &amp; Technologies &gt; CLI Templates &gt; System Templates - CLI &gt; Collecting Traffic Statistics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Voice Video: Use Medianet Perfmon CLI template. Choose Configuration &gt; Templates &gt; Features &amp; Technologies &gt; CLI Templates &gt; System Templates - CLI &gt; Medianet – PerfMon</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Format: V9</td>
<td>Netflow-Traffic-Conv-Netflow-Voice-Video-</td>
</tr>
<tr>
<td>IOS XE 3.11 to</td>
<td>TCP/UDP conversation traffic</td>
<td>TCP/UDP conversation traffic Voice &amp; Video</td>
<td>Choose Services &gt; Application Visibility &amp; Control &gt; Interfaces Configuration</td>
<td>Netflow-Traffic-Conv-Netflow-App-Traffic-</td>
</tr>
<tr>
<td>15.4(1) S, and later</td>
<td>Application Response Time (ART)</td>
<td></td>
<td>Format: V9 and IPFIX</td>
<td>Netflow-Traffic-Voice-Video-Netflow-URL-</td>
</tr>
<tr>
<td>Easy PerfMon</td>
<td>Voice &amp; Video HTTP URL visibility</td>
<td></td>
<td></td>
<td>Netflow-Aggregated-Traffic-Stats-</td>
</tr>
<tr>
<td>based config</td>
<td>Application Traffic Stats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(EzPM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IOS XE 3.9, 3.10</td>
<td>TCP/UDP conversation traffic</td>
<td>TCP/UDP conversation traffic Voice &amp; Video</td>
<td>Choose Services &gt; Application Visibility &amp; Control &gt; Interfaces Configuration</td>
<td>Netflow-Traffic-Conv-Netflow-App-Traffic-</td>
</tr>
<tr>
<td></td>
<td>Application Response Time (ART)</td>
<td></td>
<td>Format: V9 and IPFIX</td>
<td>Netflow-Voice-Video-Netflow-URL-Netflow-AVC-Troubleshooting-</td>
</tr>
<tr>
<td></td>
<td>Voice &amp; Video HTTP URL visibility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AVC Troubleshooting</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table 8-1  NetFlow Support Summary  (continued)

<table>
<thead>
<tr>
<th>Device Type</th>
<th>IOS Versions Supporting NetFlow</th>
<th>Supported NetFlow Export Types</th>
<th>NetFlow Configuration in Prime Infrastructure</th>
<th>Template Naming Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Application Response Time (ART)</td>
<td>Voice &amp; Video: Use Medianet Perfmon CLI template. Choose Configuration &gt; Templates &gt; Features &amp; Technologies &gt; CLI Templates &gt; System Templates - CLI &gt;Medianet – PerfMon</td>
<td>Netflow-Voice-Video-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voice &amp; Video</td>
<td>Format: V9</td>
<td></td>
</tr>
</tbody>
</table>
|             | 15.2(4) M and 15.3(1)T          | TCP/UDP conversation traffic    | Choose: Services > Application Visibility & Control >Interfaces Configuration | Netflow-Traffic-Conv-
|             |                                 | Application Response Time (ART) | Format: V9 and IPFIX                          | Netflow-App-Traffic-
|             |                                 | Voice & Video                   |                                               | Netflow-Voice-Video- |
|             | 15.4(1)T and later Easy PerfMon based configuration (EzPM) | TCP/UDP conversation traffic    | Choose Services > Application Visibility & Control > Interfaces Configuration | Netflow-Traffic-Conv-
|             |                                 | Application Response Time (ART) | Format: V9 and IPFIX                          | Netflow-App-Traffic-
|             |                                 | Voice & Video                   |                                               | Netflow-Voice-Video- |
|             |                                 | HTTP URL visibility             |                                               | Netflow-App-Traffic-URL- |
| Cisco Catalyst 2000 | 15.0(2) UCP and later | TCP/UDP conversation traffic    | Create a custom CLI template. See Configuring NetFlow Export on Catalyst 2000 Switches. Format: V5, V9 | Netflow-Traffic-Conv- |
| Cisco Catalyst 3750-X, 3560-X | 15.0(1)SE IP base or IP services feature set and equipped with the network services module. | TCP/UDP conversation traffic    | Create a custom CLI template. See Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches Format: V9 | Netflow-Traffic-Conv- |
### Table 8-1  NetFlow Support Summary (continued)

<table>
<thead>
<tr>
<th>Device Type</th>
<th>IOS Versions Supporting NetFlow</th>
<th>Supported NetFlow Export Types</th>
<th>NetFlow Configuration in Prime Infrastructure</th>
<th>Template Naming Convention</th>
</tr>
</thead>
</table>
To manually configure NetFlow export on Catalyst 2000 devices, create a user-defined CLI template as shown in the following steps.

**Step 1**
Choose **Configuration > Templates > Features & Technologies > CLI Templates > CLI**.

**Step 2**
Hover your mouse cursor over the information icon and click **New** to create a new CLI template.

**Step 3**
Enter a name for the new CLI template (for example, “Prime_NF_CFG_CAT2K”).

**Step 4**
From the **Device Type** list, choose **Switches and Hubs**.

**Step 5**
In the **Template Detail > CLI Content** text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example):

```plaintext
global

flow record PrimeNFRec
  match ipv4 protocol
tcp/udp conversation
  match ipv4 source address
  voice & video
  match ipv4 destination address
  match transport source-port
  collect counter bytes long
  collect counter packets long

flow exporter PrimeNFExp
destination 172.18.54.93
  transport udp 9991
  option exporter-stats timeout 20

flow monitor PrimeNFMon
  record PrimeNFRec
  exporter PrimeNFExp

interface GigabitEthernet3/0/1
  ip flow monitor PrimeNFMon input
```

**Configuring NetFlow Export on Catalyst 2000 Switches**

To manually configure NetFlow export on Catalyst 2000 devices, create a user-defined CLI template as shown in the following steps.
Setting Up Assurance for Performance Monitoring

Chapter 8      Setting Up Network Monitoring

Setting Up Assurance for Performance Monitoring

Step 6  Click Save as New Template. After you save the template, deploy it to your devices (see Creating Feature-Level Configuration Templates).

Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches

To manually configure NetFlow to export TCP and UDP traffic on Catalyst 3000, 4000, or 6000 devices, create a user-defined CLI template as shown in the following steps.

Step 1  Choose Configuration > Templates > Features & Technologies > CLI Templates > CLI.
Step 2  Hover your mouse cursor over the information icon and click New to create a new CLI template.
Step 3  Enter a name for the new CLI template (for example, “Prime_NF_CFG_CAT3K_4K”).
Step 4  From the Device Type list, choose Switches and Hubs.
Step 5  In the Template Detail > CLI Content text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example):

```
flow record PrimeNFRec
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect counter bytes long
  collect counter packets long
!
!
flow exporter PrimeNFExp
  destination 172.18.54.93
  transport udp 9991
  option exporter-stats timeout 20
!
!
flow monitor PrimeNFMon
  record PrimeNFRec
  exporter PrimeNFExp

interface GigabitEthernet3/0/1
  ip flow monitor PrimeNFMon input
```

Step 6  Click Save as New Template. After you save the template, deploy it to your devices (see Creating Feature-Level Configuration Templates).
Configuring NetFlow on ISR Devices

To manually configure NetFlow to export MACE traffic on an ISR device, use the following steps to create a user-defined CLI template:

**Step 1** Choose Configuration > Templates > Features & Technologies > CLI Templates > CLI.

**Step 2** Hover your mouse cursor over the information icon and click New to create a new CLI template.

**Step 3** Enter a name for the new CLI template (for example, “Prime_NF_CFG_MACE”).

**Step 4** From the Device Type list, choose Routers.

**Step 5** In the Template Detail > CLI Content text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example)

```
flow record type mace mace-record
collect application name
collect art all
!
flow exporter mace-export
destination <PI_SERVER_IP_ADDRESS>
source GigabitEthernet0/1
transport udp 9991
!
flow monitor type mace mace-monitor
record mace-record
exporter mace-export
cache timeout update 600

class-map match-all PrimeNFClass
    match protocol ip
    exit

policy-map type mace mace_global
class PrimeNFClass
flow monitor mace-monitor
exit
exit

interface GigabitEthernet 0/1
mace enable
```

**Step 6** Click Save as New Template. After you save the template, deploy it to your devices (see Creating Feature-Level Configuration Templates).
Changing User Settings

Setting User Preferences

Prime Infrastructure provides user preference settings that allows you to modify how information is displayed.

- Changing Your User Preferences
- Changing Your Idle-User Timeout
- Changing List Length

Changing Your User Preferences

To change your user preferences, click the Settings icon (the gear icon on the right side of the menu bar) and choose My Preferences and change the settings shown on the My Preferences page.

Related Topics

- Changing Your Idle-User Timeout
- Changing List Length
- Changing Alarm Display Behavior
- Customizing the Alarm Summary
- Toolbar

Changing Your Idle-User Timeout

Prime Infrastructure provides two settings that control when and how idle users are automatically logged out:

- User Idle Timeout—You can disable or configure this setting, which ends your user session automatically when you exceed the timeout. It is enabled by default and is set to 10 minutes.
- Global Idle Timeout—The Global Idle Timeout setting overrides the User Idle Timeout setting. The Global Idle Timeout is enabled by default and is set to 10 minutes. Only users with administrative privileges can disable the Global Idle Timeout setting or change its time limit.
You may find it useful to disable the user idle timeout feature if, for example, you are an Operations Center user experiencing sudden log-offs, due to idle sessions, with one or more Prime Infrastructure instances managed by Operations Center. For details, see “Disabling Idle User Timeout for Operations Center” in Related Topics.

To change the timeout settings, follow these steps:

**Step 1** Click the **Settings** icon and choose **My Preferences**.

**Step 2** Under **User Idle Timeout**:
- Change the check status of the check box next to **Logout idle user** to enable or disable your idle timeout.
- From the **Logout idle user after** drop-down list, choose one of the idle timeout limits.

**Step 3** Click **Save**. You will need to log out and log back in for this change to take effect.

**Related Topics**
- Changing Your User Preferences
- Disabling Idle User Timeout for Operations Center
- Changing the Global Idle Timeout

### Changing List Length

Prime Infrastructure lets you change the default number of entries displayed in some lists. The Items Per List setting affects the number of entries displayed on the monitoring pages for:
- APs
- Controllers
- Site Maps
- Mesh
- CleanAir

The Items Per List setting does not apply to Network Devices, alarms and events, configuration archive, software image management, or configuration.

The default number of items to shown on a given page is 50.

**Step 1** Click the **Settings** icon and choose **My Preferences**.

**Step 2** Change the setting in the **Items Per List Page** drop down.

**Step 3** Click **Save**.

**Related Topic**
- Changing Your User Preferences
Viewing and Managing Dashboards

Dashboards display at-a-glance views of the most important data in your network. They provide status and alerts, monitoring, and reporting information. You can also create a custom dashboard that contains only the information that is most important to you. To get a quick overall view of your network, you can specify a specific dashboard as your homepage by Prime Infrastructure by choosing Help > Getting Started, and then clicking Save and Launch Homepage under the dashboard you want to set as your homepage.

Related Topics
- Types of Dashboards
- Viewing Options for Metrics
- Managing and Editing Dashboards
- Adding Dashboards
- Adding Dashlets

Types of Dashboards

Prime Infrastructure provides several types of dashboards that contain graphs and visual indicators:
- Network Summary—Provides an overview summary of your network including status metrics and a tab specific to incidents which includes alarm and event type graphs and critical, major, and minor alarm counts.
- Overview—Provides summary information and includes tabs specific to alarms and events, clients, network devices, network interfaces, and service assurance.
- Performance—Provides a summary of performance metrics and includes tabs specific to sites, devices, access points, interfaces, applications, voice/video, end user experience, and WAN optimization.
- Data Center—Provides information about Data Center and includes tabs specific to Compute and Host.

Most dashboards contain metrics at the top of the window.
Types of Dashboards

Note
Prime Infrastructure filters the monitoring data for virtual domains, based on the end points assigned to the sites and not based on the datasource, hence the dashboards display information for all virtual domains, irrespective of the virtual domain assigned to the user.

Related Topics
- Network Summary Dashboards
- Overview Dashboards
- Wireless Dashboards
- Performance Dashboards
- Data Center Dashboards
- Viewing Options for Metrics

Network Summary Dashboards

Choose one of the following dashboards under Dashboard > Network Summary to view a summary of important data points in your network. Table 10-1 describes the default information shown in each of the dashboards under Dashboard > Network Summary.

Table 10-1  Network Summary Dashboard Descriptions

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Network Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall system health such as</td>
<td>Overview</td>
<td></td>
</tr>
<tr>
<td>• Reachability metrics for ICMP, APs, and controllers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Alarm summary metrics for all alarms and rogue alarms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Health metrics for system health, WAN link health, and service health</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Coverage areas, including links to APs not assigned to map</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Client counts by association/authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Top CPU, interface, and memory utilization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Network topology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Alarm summary metrics for all alarms and rogue alarms</td>
<td>Incidents</td>
<td></td>
</tr>
<tr>
<td>• Health metrics for system health, WAN link health, and service health</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Alarms graph</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Top alarm and event types graphs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 10  Viewing and Managing Dashboards

Table 10-1  Network Summary Dashboard Descriptions

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Network Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site health such as</td>
<td>Site Summary</td>
</tr>
<tr>
<td>• Top N applications</td>
<td></td>
</tr>
<tr>
<td>• Top N clients</td>
<td></td>
</tr>
<tr>
<td>• Top N devices with the most alarms</td>
<td></td>
</tr>
<tr>
<td>• Top N servers</td>
<td></td>
</tr>
<tr>
<td>Network health shown in a map view or as a table which displays information about the</td>
<td>Network Health</td>
</tr>
<tr>
<td>health metrics for each network element and the criticality of each metric for a specified</td>
<td></td>
</tr>
<tr>
<td>period of time.</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

• Network Summary Dashboard Features
• Viewing Options for Metrics
• Managing and Editing Dashboards
• Troubleshooting Network Health Using Dashboards

Network Summary Dashboard Features

When you choose a dashboard under Dashboard > Network Summary, you can perform any of the following actions:

• To rename the dashboard, click on the dashboard name in the tab, then enter a new name.
• To view help text, hover your cursor over the Help icon next to any metric name.
• To modify what dashboard is displayed by default when you choose Dashboard > Network Summary, click on the dashboard you want displayed as default, then click Manage Dashboards > Mark as Default Dashboard.
• To export an entire Network Summary dashboard including all data shown on the page, click Settings > Export. You can export the data in CSV or PDF format.
• To add a dashlet to any dashboard, select Settings > Add Dashlet(s). On Network Summary dashboards, you can add dashlets from any category. Use the search field to search for a particular dashlet you want to add.

The toolbar for Network Summary Dashboards is shown in Figure 10-1:

Figure 10-1  Network Summary Dashlet Icons
Table 10-2 Overview Dashboard Descriptions

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Overview &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Network device summary graph, including the reachable and unreachable devices</td>
<td>General</td>
</tr>
<tr>
<td>• Top N CPU and memory utilization</td>
<td></td>
</tr>
<tr>
<td>• Client count by association/authentication</td>
<td></td>
</tr>
<tr>
<td>• Coverage area</td>
<td></td>
</tr>
<tr>
<td>• Top N sites with the most alarms</td>
<td>Incidents</td>
</tr>
<tr>
<td>• Alarm summary graph</td>
<td></td>
</tr>
<tr>
<td>• Alarm type graph</td>
<td></td>
</tr>
<tr>
<td>• Device reachability status</td>
<td></td>
</tr>
<tr>
<td>• Syslog summary and watch</td>
<td></td>
</tr>
<tr>
<td>• Client troubleshooting tool</td>
<td>Client</td>
</tr>
<tr>
<td>• Wired client speed distribution graph</td>
<td></td>
</tr>
<tr>
<td>• Client distribution graph</td>
<td></td>
</tr>
<tr>
<td>• Client alarms and events summary</td>
<td></td>
</tr>
<tr>
<td>• Client traffic graph</td>
<td></td>
</tr>
<tr>
<td>• Top 5 SSIDs by client count</td>
<td></td>
</tr>
<tr>
<td>• Top 5 switches by client count</td>
<td></td>
</tr>
<tr>
<td>• Client posture status</td>
<td></td>
</tr>
<tr>
<td>• Top N CPU and memory utilization</td>
<td>Network Devices</td>
</tr>
<tr>
<td>• Top N environmental temperature</td>
<td></td>
</tr>
</tbody>
</table>
Table 10-2   Overview Dashboard Descriptions

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Overview &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Interface availability summary</td>
<td>Network Interface</td>
</tr>
<tr>
<td>• Top N interface utilization</td>
<td></td>
</tr>
<tr>
<td>• Interface utilization summary graph</td>
<td></td>
</tr>
<tr>
<td>• Top N interface errors and discards</td>
<td></td>
</tr>
<tr>
<td>• Top N applications</td>
<td></td>
</tr>
<tr>
<td>• Top N servers</td>
<td></td>
</tr>
<tr>
<td>• Top N resources by NetFlow</td>
<td></td>
</tr>
<tr>
<td>• Top N clients</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Managing and Editing Dashboards
- Viewing Options for Metrics

Wireless Dashboards

Table 10-3 describes the default information shown in each of the dashboards under Dashboard > Wireless.

Table 10-3   Wireless Dashboard Descriptions

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Wireless &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Index, including the top security issues</td>
<td>Security</td>
</tr>
<tr>
<td>• Adaptive WIPS</td>
<td></td>
</tr>
<tr>
<td>• Rogue classification graph</td>
<td></td>
</tr>
<tr>
<td>• Rogue containment graph</td>
<td></td>
</tr>
<tr>
<td>• Attacks detected</td>
<td></td>
</tr>
<tr>
<td>• Malicious, unclassified, friendly, and custom rogue APs</td>
<td></td>
</tr>
<tr>
<td>• CleanAir security</td>
<td></td>
</tr>
<tr>
<td>• Adhoc rogues</td>
<td></td>
</tr>
<tr>
<td>• Most recent mesh alarms</td>
<td>Mesh</td>
</tr>
<tr>
<td>• Mesh work node hop count</td>
<td></td>
</tr>
<tr>
<td>• Mesh worst SNR link</td>
<td></td>
</tr>
<tr>
<td>• Mesh worst packet error rate</td>
<td></td>
</tr>
</tbody>
</table>
Types of Dashboards

Performance Dashboards

Choose one of the dashboards under Dashboard > Performance to view a summary of performance metrics. Viewing the performance dashboards can show you the health of the networks, servers, and applications.

You can use performance graphs to compare the performance of different devices or interfaces. Table 10-4 describes the default information shown in each of the dashboards under Dashboard > Performance.

---

Table 10-3  Wireless Dashboard Descriptions

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Wireless &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>CleanAir</td>
</tr>
<tr>
<td>The information in the worst interferer and interferer count charts is collected from the mobility services engines (MSE). If MSEs are not available, this chart does not show any results.</td>
<td></td>
</tr>
<tr>
<td>• 802.11 average and minimum air quality</td>
<td></td>
</tr>
<tr>
<td>• Worst interferers</td>
<td></td>
</tr>
<tr>
<td>• Interferer count</td>
<td></td>
</tr>
<tr>
<td>• Recent security-risk interferers</td>
<td></td>
</tr>
<tr>
<td>• Recent CAS notifications for interferers</td>
<td></td>
</tr>
<tr>
<td>• MSE historical element count</td>
<td>ContextAware</td>
</tr>
<tr>
<td>• Rogue elements detected by CAS</td>
<td></td>
</tr>
<tr>
<td>• Location assisted client troubleshooting</td>
<td></td>
</tr>
<tr>
<td>• MSE tracking counts</td>
<td></td>
</tr>
<tr>
<td>• Top 5 MSEs</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Managing and Editing Dashboards
- Viewing Options for Metrics
### Table 10-4  Performance Dashboard Descriptions

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Performance &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the specified site:</td>
<td>Site</td>
</tr>
<tr>
<td>- Client traffic (regular and optimized)</td>
<td></td>
</tr>
<tr>
<td>- Device with most alarms</td>
<td></td>
</tr>
<tr>
<td>- Top N applications</td>
<td></td>
</tr>
<tr>
<td>- Device reachability status</td>
<td></td>
</tr>
<tr>
<td>For the specified device:</td>
<td>Device</td>
</tr>
<tr>
<td>- Device Availability Trend</td>
<td></td>
</tr>
<tr>
<td>- Device memory and CPU utilization trend</td>
<td></td>
</tr>
<tr>
<td>- Device Port Summary</td>
<td></td>
</tr>
<tr>
<td>- Device Health Information</td>
<td></td>
</tr>
<tr>
<td>- Top N Interfaces by Netflow</td>
<td></td>
</tr>
<tr>
<td>For the specified access point:</td>
<td>Access Point</td>
</tr>
<tr>
<td>- Access point details</td>
<td></td>
</tr>
<tr>
<td>- Top clients and applications</td>
<td></td>
</tr>
<tr>
<td>- Channel utilization</td>
<td></td>
</tr>
<tr>
<td>- Client count</td>
<td></td>
</tr>
<tr>
<td>For the specified interface:</td>
<td>Interface</td>
</tr>
<tr>
<td>- Interface details</td>
<td></td>
</tr>
<tr>
<td>- Interface Availability Trend</td>
<td></td>
</tr>
<tr>
<td>- Interface In and Out Errors and Discards</td>
<td></td>
</tr>
<tr>
<td>- Interface Tx and Rx utilization</td>
<td></td>
</tr>
<tr>
<td>- Top applications and clients</td>
<td></td>
</tr>
<tr>
<td>- Top application traffic over time</td>
<td></td>
</tr>
<tr>
<td>- Number of clients over time</td>
<td></td>
</tr>
<tr>
<td>- DSCP classification</td>
<td></td>
</tr>
<tr>
<td>- QoS class map statistics</td>
<td></td>
</tr>
<tr>
<td>- Top QoS class map statistics trend</td>
<td></td>
</tr>
<tr>
<td>For the specified application:</td>
<td>Application</td>
</tr>
<tr>
<td>- Top clients and servers</td>
<td></td>
</tr>
<tr>
<td>- Application traffic analysis graph</td>
<td></td>
</tr>
<tr>
<td>- Application server performance</td>
<td></td>
</tr>
<tr>
<td>- Top interfaces over time</td>
<td></td>
</tr>
<tr>
<td>- Top RTP streams</td>
<td>Voice/Video</td>
</tr>
<tr>
<td>- Worst RTP streams by packet loss</td>
<td></td>
</tr>
<tr>
<td>- Works site-to-site connections by KPI</td>
<td></td>
</tr>
</tbody>
</table>
Table 10-4 Performance Dashboard Descriptions (continued)

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Performance &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the specified client:</td>
<td>End User Experience</td>
</tr>
<tr>
<td>• Top applications</td>
<td></td>
</tr>
<tr>
<td>• User sites summary</td>
<td></td>
</tr>
<tr>
<td>• Client traffic</td>
<td></td>
</tr>
<tr>
<td>• Multi-segment analysis</td>
<td>WAN Optimization</td>
</tr>
<tr>
<td>• Traffic volume and compression ration</td>
<td></td>
</tr>
<tr>
<td>• Transaction time</td>
<td></td>
</tr>
<tr>
<td>• Average concurrent connections (optimized versus pass-through)</td>
<td></td>
</tr>
<tr>
<td>• Multi-segment network time</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
• Managing and Editing Dashboards
• Viewing Options for Metrics

Data Center Dashboards

Table 10-5 describes the default information shown in each of the dashboards under Dashboard > Data Center.

Table 10-5 Data Center Dashboard Descriptions

<table>
<thead>
<tr>
<th>To View This Information</th>
<th>Chose Dashboard &gt; Data Center &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the specified data center:</td>
<td>Compute</td>
</tr>
<tr>
<td>• Virtual machine summary by OS</td>
<td></td>
</tr>
<tr>
<td>• Virtual machine resource usage summary</td>
<td></td>
</tr>
<tr>
<td>• Compute resource summary</td>
<td></td>
</tr>
<tr>
<td>• Top 5 host usage summary by CPU</td>
<td></td>
</tr>
<tr>
<td>For the specified host:</td>
<td>Host</td>
</tr>
<tr>
<td>• Host CPU usage</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
• Managing and Editing Dashboards
• Viewing Options for Metrics

Managing and Editing Dashboards

The Prime Infrastructure dashboards contain dashlets with charts, graphs, tables, and other information. There are various tools, options, and settings you can specify in order to customize the dashboards.
Related Topics
- Viewing Options for Metrics
- Understanding Dashlet Icons
- Adding Dashboards
- Adding Dashlets
- Time Filters for Dashboards and Dashlets
- Overriding a Dashlet Filter
- Creating Generic Dashlets

Viewing Options for Metrics

You can perform the following actions on the Metrics, which are displayed at the top of most dashboards:
- Add or remove metrics by selecting Settings > Add or Remove Metric Dashlet(s).
- Reorder the metrics by clicking near the metric title and dragging and dropping it to the area you prefer.
- Click any of the hyperlinked numbers in any of the boxes to go to the details for that metric. For example, if you click on a number displayed in the Alarm Summary metrics, you go to the alarm page to view more information about the alarm(s).

Related Topic
- Managing and Editing Dashboards

Understanding Dashlet Icons

Dashboards contain dashlets that consist of visual displays such as tables and charts. You can drag and drop dashlets to any location in the dashboards. Hover your mouse cursor over any dashlet, and the following icons appear in the top-right corner of the dashboard.

![Figure 10-2 Dashlet Icons](image)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dashlet options include editing the dashlet title, refreshing the dashlet, or changing the dashlet refresh interval. (To disable refresh, unselect Refresh Dashlet.)</td>
</tr>
<tr>
<td>2</td>
<td>Dashlet help includes a picture of the dashlet, a description, the data sources used to populate the dashlet, and any filters you can apply to the dashlet’s data.</td>
</tr>
<tr>
<td>3</td>
<td>Refresh the dashlet.</td>
</tr>
<tr>
<td>4</td>
<td>Maximize the dashlet. A restore icon appears, allowing you to restore the dashlet to its default size.</td>
</tr>
</tbody>
</table>
Dashlet badges indicate which filters were applied when generating the contents of each dashlet.

Figure 10-3   Dashlet Badges

1  Network aware filter. Use this filter to collect data for all devices, wired devices, wireless devices, or a specific wireless SSID.
2  Site filter. Use this filter to collect data associated with an AP or a controller located at a predefined location.
3  Application filter. Use this filter to collect data based on a service, an application within a service, up to ten separate applications, or all applications.
4  Time frame filter. Use this filter to collect data for a preset time period, or you can specify a beginning and ending date.

You can customize the predefined set of dashlets depending on your network management needs. You can organize the information in user-defined dashboards. The default view comes with default dashboards and pre-selected dashlets for each.

When using dashlets bear in mind:

- The label “Edited” next to the dashlet heading indicates that the dashlet has been customized. If you reset to the default settings, the Edited label is cleared.
- When an upgrade occurs, the arrangement of dashlets in a previous version is maintained. Because of this, dashlets or features added in a new release are not displayed. Click the Manage Dashboards link to discover new dashlets.
- The horizontal and vertical scrollbars are visible if you zoom the dashlets. Reset the zoom level back to zero, or no zoom for viewing the dashlets without the scrollbars.

Related Topics
- Adding Dashboards
- Restoring Dashboards
- Adding Dashlets

Adding Dashboards

Prime Infrastructure has a set of default dashboards. You can also create a custom dashboard to display information specific to your needs:
**Adding Dashlets**

Each dashboard displays a subset of the available dashlets. You can add any dashlet that is not automatically displayed to any dashboard you want.

**Step 1** Choose **Dashboard**, then select the dashboard to which you want to add the dashlet.
**Step 2** Click the **Settings** icon, then choose **Add Dashlets**.
**Step 3** Find the dashboard heading in the drop-down list; you can add any of the dashlets under that heading to that dashboard.

**Related Topic**
- Default Dashlets

**Table 10-6 Default General Dashlets**

<table>
<thead>
<tr>
<th>Dashlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Join Taken Time</td>
<td>Displays the access point name and the amount of time (in days, minutes, and seconds) that it took for the access point to join.</td>
</tr>
<tr>
<td>Top N APs by Channel Utilization</td>
<td>Shows the top N APs with maximum channel utilization.</td>
</tr>
<tr>
<td>AP Uptime</td>
<td>Displays each access point name and amount of time it has been associated.</td>
</tr>
<tr>
<td>CAPWAP Uptime</td>
<td>Shows the APs based on the CAPWAP uptime.</td>
</tr>
<tr>
<td>Coverage Areas</td>
<td>Displays the list coverage areas and details about each coverage area.</td>
</tr>
<tr>
<td>Device Unreachability Summary</td>
<td>Displays the unreachability summary of APs, routers, and switches.</td>
</tr>
<tr>
<td>Network Topology</td>
<td>Displays the network topology map.</td>
</tr>
</tbody>
</table>
Chapter 10      Viewing and Managing Dashboards

Adding Dashlets

Table 10-6  Default General Dashlets (continued)

<table>
<thead>
<tr>
<th>Dashlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unreachable MA-MC CAPWAP Tunnels</td>
<td>Displays the unreachability status between the mobility agent and mobility controller.</td>
</tr>
<tr>
<td>Device Uptime</td>
<td>Displays the devices based on the device uptime.</td>
</tr>
<tr>
<td>Ad hoc Rogues</td>
<td>Displays ad hoc rogues for the previous hour, previous 24 hours, and total active.</td>
</tr>
<tr>
<td>GETVPN Network Statistics</td>
<td>Shows available GETVPN network groups summary.</td>
</tr>
<tr>
<td>Job Information Status</td>
<td>Shows all user defined jobs.</td>
</tr>
<tr>
<td>Most Recent AP Alarms</td>
<td>Displays the five most recent access point alarms. Click the number in parentheses to open the Alarms page which shows all alarms.</td>
</tr>
<tr>
<td>Network Device Summary</td>
<td>Displays the total managed device count, number of available access points (APs) and total count of managed unreachable devices in the network.</td>
</tr>
</tbody>
</table>

The Unified AP Reachability can be any of the following:

- Reachable—Operational status is registered and admin status is enable.
- Unreachable—Operational status unregistered and admin status is enable.

The network device summary dashlet for AP devices will be displayed only if the admin status is enabled.

The AP reachability information is defined as follows:

- Unified AP—Reachability is defined by the Operational Status. If the AP is registered to a wireless LAN controller, it is considered reachable. If it is not registered, it is not reachable.
- Autonomous AP—Reachability is defined by the device’s SNMP Reachability field in the Device Work Center.

Recent Alarms                  | Displays the five most recent alarms by default. Click the number in parentheses to open the Alarms page.                                |

Recent Coverage Holes          | Displays the recent coverage hole alarms listed by access point.                                                                         |

Software Summary               | Displays the software version and software type of all managed devices.                                                                     |

Table 10-7 lists the default Security Dashlets that you can add in your Prime Infrastructure home page.

Table 10-7  Default Security Dashlets

<table>
<thead>
<tr>
<th>Dashlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Classification</td>
<td>Allows you to classify the clients that are added in Prime Infrastructure.</td>
</tr>
</tbody>
</table>
Table 10-8 lists the default Client Dashlets that you can add in your Prime Infrastructure home page.

**Table 10-8  Default Client Dashlets**

| Dashlet                          | Description                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
| Client Troubleshooting Dashlet   | Allows you to enter a Client MAC address and starts the client troubleshooting tool.                                                                                                                                                                                                                                                                                  |
| Client Distribution Dashlet      | Shows the client distribution by protocol, EAP type, and authentication type. You can click a protocol to access the list of users belonging to that protocol. For example, if you click the 802.3 protocol, you can directly access the list of the wired clients and users in the Clients and Users page. |
| Client Alarms and Events Summary | Shows the most recent client alarms of both wired and wireless clients.                                                                                                                                                                                                                                                                                             |
|                                  | - Client Association Failure                                                                                                                                                                                                                                                                                                                                        |
|                                  | - Client Authentication Failure                                                                                                                                                                                                                                                                                                                                 |
|                                  | - Client WEP Key Decryption Error                                                                                                                                                                                                                                                                                                                                |
|                                  | - Client WPA MIC Error Counter Activated                                                                                                                                                                                                                                                                                                                          |
|                                  | - Client Excluded                                                                                                                                                                                                                                                                                                                                                 |
|                                  | - Autonomous AP Client Authentication Failure                                                                                                                                                                                                                                                                                                                     |
|                                  | - Wired Client Authentication Failure                                                                                                                                                                                                                                                                                                                            |
|                                  | - Wired Client Authorization Failure                                                                                                                                                                                                                                                                                                                             |
|                                  | - Wired Client Critical VLAN Assigned                                                                                                                                                                                                                                                                                                                           |
|                                  | - Wired Client Auth fail VLAN Assigned                                                                                                                                                                                                                                                                                                                          |
|                                  | - Wired Client Guest VLAN Assigned                                                                                                                                                                                                                                                                                                                               |
|                                  | - Wired Client Security Violation                                                                                                                                                                                                                                                                                                                                |
| Wireless Client Traffic Dashlet  | Reports the amount of bandwidth that client traffic is consuming for each network protocol used by the clients to connect to the network.                                                                                                                                                                                                                               |
| Wired Client Speed Distribution  | Shows the wired client speeds and the client count for each speed. There are three different speeds on which clients run:                                                                                                                                                                                                                                           |
| Dashlet                          | - 10 Mbps                                                                                                                                                                                                                                                                                                                                                       |
|                                  | - 100 Mbps                                                                                                                                                                                                                                                                                                                                                      |
|                                  | - 1 Gbps                                                                                                                                                                                                                                                                                                                                                        |
|                                  | The ports are in the Auto Negotiate mode by default. For example, you get 100 Mbps speed for a client that runs in 100 Mbps speed.                                                                                                                                                                                                                                       |
| Top 5 SSIDs by Client Count      | Shows the count of currently associated and authenticated clients. You can choose to display the information in table form or in an area chart.                                                                                                                                                                                                                      |
| Top 5 Switches by Switch Count   | Displays the five switches that have the most clients as well as the number of clients associated to the switch.                                                                                                                                                                                                                                                  |
### Adding Dashlets

Client Posture Status Dashlet
Prime Infrastructure collects the posture status information from the Identity Services Engine (ISE). You need to add an ISE for authorization and authentication purpose. After you enable necessary functions in ISE, Prime Infrastructure shows the data in the Client Posture Status dashlet.

This dashlet displays the client posture status and the number of clients in each of the following status categories:
- Compliant
- Non-compliant
- Unknown
- Pending
- Not Applicable
- Error

<table>
<thead>
<tr>
<th>Dashlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Count by IP Address Type</td>
<td>Displays a chart which shows client count trend over time by different IP addresses types. The types include IPv4, IPv6, Dual-Stack and Unknown.</td>
</tr>
<tr>
<td>IPv6 Assignment Distribution</td>
<td>Displays a pie chart which shows distribution of all clients based on how their IPv6 addresses get assigned. The type include Unknown, DHCPv6, Self-Assigned, and SLACC or Static.</td>
</tr>
<tr>
<td>User Auth Failure Count</td>
<td>Displays a chart which shows user authentication failure count trend over time.</td>
</tr>
<tr>
<td>Client Protocol Distribution</td>
<td>Displays the current client count distribution by protocols.</td>
</tr>
<tr>
<td>Client EAP Type Distribution</td>
<td>Displays the count based on the EAP type.</td>
</tr>
<tr>
<td>Guest Users Count</td>
<td>Displays Guest client count over a specified time.</td>
</tr>
<tr>
<td>Client CCX Distribution</td>
<td>Displays a pie chart which shows client distribution among different CCX versions.</td>
</tr>
<tr>
<td>Top N Client Count</td>
<td>Displays a bar chart which shows top N elements based on client count. The elements include SSID, APs, Controller, Endpoint Type, Vendor, Switches, and Anchor Controllers. It is a generic top N chart to replace different individual top N charts. The Top N Client Count shows the anchor clients count on each anchor controller.</td>
</tr>
<tr>
<td>Client Mobility Status Distribution</td>
<td>Displays a pie chart which shows client distribution between local (not anchored) and anchored.</td>
</tr>
<tr>
<td>Client 11u Distribution</td>
<td>Displays a pie chart which shows 11u clients over non-11u clients.</td>
</tr>
<tr>
<td>11u Client Count</td>
<td>Displays a pie chart which shows 11u clients over non-11u clients.</td>
</tr>
<tr>
<td>11u Client Traffic</td>
<td>Displays a chart which shows 11u client traffic trend over time.</td>
</tr>
<tr>
<td>PMIP Clients Distribution</td>
<td>Displays a pie chart which shows PMIP client over non-PMIP clients.</td>
</tr>
<tr>
<td>PMIP Client Count</td>
<td>Displays a chart which shows PMIP client count trend over time.</td>
</tr>
<tr>
<td>Top APs by Client Count</td>
<td>Displays the Top APs by client count.</td>
</tr>
<tr>
<td>Most Recent Client Alarms</td>
<td>Displays the most recent client alarms.</td>
</tr>
<tr>
<td>Recent 5 Guest User Accounts</td>
<td>Displays the most recent guest user accounts created or modified</td>
</tr>
<tr>
<td>Latest 5 logged in Guest Users</td>
<td>Displays the most recent guest users to log in.</td>
</tr>
<tr>
<td>Clients Detected by Context Aware Service</td>
<td>Displays the client count detected by the context aware service within the previous 15 minutes.</td>
</tr>
</tbody>
</table>
### Table 10-8  Default Client Dashlets (continued)

<table>
<thead>
<tr>
<th>Dashlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Authentication Type Distribution</td>
<td>Displays the client count based on the type of client authentication.</td>
</tr>
<tr>
<td>Client Count By Association/Authentication</td>
<td>Shows client count over a specified time interval. Count can be based on associated or authenticated clients.</td>
</tr>
<tr>
<td>Client Count By Wired/Wireless</td>
<td>Shows client count for wireless, wired or a combination of both.</td>
</tr>
<tr>
<td>Client Traffic By IP Address Type</td>
<td>Shows client traffic based on IP address type.</td>
</tr>
<tr>
<td>IP Address Type Distribution</td>
<td>Shows client distribution based on IP address type.</td>
</tr>
</tbody>
</table>

### Table 10-9  Default Network Dashlets

<table>
<thead>
<tr>
<th>Dashlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Utilization Summary</td>
<td>Displays the distribution of devices by CPU utilization across 4 CPU utilization bands (0-25%, 26-50%, 51-75%, 76-100%)</td>
</tr>
<tr>
<td>Device Availability Summary</td>
<td>Shows a summary, total device count and pie chart distribution of devices in a given site that are reachable (and Unreachable) through SNMP.</td>
</tr>
<tr>
<td>Interface Availability Summary</td>
<td>Shows the availability of the interface in percentage in the selected time range.</td>
</tr>
<tr>
<td>Interface Statistics</td>
<td>Shows the statistics information of the interface in a given site.</td>
</tr>
<tr>
<td>Interface Statistics Summary</td>
<td>Shows the total count of interfaces and a pie chart distribution of interface status (Up, Operationally Up, Administratively Down) in a given site.</td>
</tr>
<tr>
<td>Interface Utilization Summary</td>
<td>Shows pie chart distribution of devices by interface utilization across 4 Interface Utilization bands (0-25%, 25-50%, 51-75%, 75-100%) in a given site. The inner pie represents the received (Rx) utilization and the outer pie represents transmitted (Tx) utilization.</td>
</tr>
<tr>
<td>Top N CPU Utilization</td>
<td>Shows the top N devices with maximum CPU utilization.</td>
</tr>
<tr>
<td>Top N Environmental Temperature</td>
<td>Shows the top N tabulated list of average, maximum, minimum, current temperature associated with devices in the network. For the stacked switches, the device name will be appended with switch instance. For example: RB-Edison.Cisco.com-Switch-1, where Switch-1 is switch instance.</td>
</tr>
<tr>
<td>Top N Interface Errors and Discards</td>
<td>Displays the top N interfaces with highest input and output errors and discards.</td>
</tr>
<tr>
<td>Top N Interface Utilization</td>
<td>Shows pie chart distribution of devices by interface utilization-transmitted across 4 Interface Utilization bands (0-25%, 25-50%, 51-75%, 75-100%) in a given site.</td>
</tr>
<tr>
<td>Top N Memory Utilization</td>
<td>Shows the tabulated list of top N memory utilization in the network.</td>
</tr>
</tbody>
</table>
Table 10-10 lists the default Service Assurance Dashlets that you can add in your Prime Infrastructure home page.

Table 10-10  Default Service Assurance Dashlets

<table>
<thead>
<tr>
<th>Dashlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top N Applications</td>
<td>Shows top N applications with break down of wired/wireless/unknown in terms of total traffic volume/rate for a site/enterprise, client, and interface.</td>
</tr>
<tr>
<td>TOP N Clients</td>
<td>Shows top N clients based on total traffic volume/rate for site/enterprise and application, service or a set of applications.</td>
</tr>
<tr>
<td>Top N Interfaces by Netflow</td>
<td>Shows the top N interfaces with Netflow traffic based on volume.</td>
</tr>
<tr>
<td>Top N Resources by Netflow</td>
<td>Shows the Top N devices that are exporting Netflow traffic by volume or rate. It provides a toggle between Netflow exporting devices and sites with Netflow data. In Root Domain device list in the dashlet will not be VD aware.</td>
</tr>
<tr>
<td>Top N Servers</td>
<td>Shows Top N Servers by traffic rate.</td>
</tr>
<tr>
<td>Top N Sites by PFR</td>
<td>This dashlet lists the Top N Sites with the most Pfr, out of policy counts in the selected time range</td>
</tr>
<tr>
<td>Top N WAN Interface</td>
<td>Shows the tabulated list of Top N WAN Interface utilization in the network.</td>
</tr>
<tr>
<td>Worst N Sites by MOS</td>
<td>Shows the worst sites by MOS score.</td>
</tr>
<tr>
<td>Worst N sites by Transaction Time</td>
<td>Shows site to site average transaction time for an application, service or a set of applications.</td>
</tr>
</tbody>
</table>

Table 10-11 lists the default Incident Dashlets that you can add in your Prime Infrastructure home page.

Table 10-11  Default Incident Dashlets

<table>
<thead>
<tr>
<th>Dashlet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Summary</td>
<td>Shows a pie chart distribution of alarms for Switches and Hubs, Ad hoc Rogue, Routers, AP, System, Rogue AP etc.</td>
</tr>
<tr>
<td>Device Reachability Summary</td>
<td>This dashlet shows a tabulated view of each device's SNMP reachability status.</td>
</tr>
<tr>
<td>Top N Alarm Types</td>
<td>Shows a horizontal bar chart of the top N alarm types with their associate counts.</td>
</tr>
<tr>
<td>Top N Events</td>
<td>Shows a horizontal bar chart of the events types and their counts.</td>
</tr>
<tr>
<td>Top N Sites with Most Alarms</td>
<td>Shows a horizontal bar chart of the top N sites with highest alarm counts.</td>
</tr>
<tr>
<td>Top N Syslog Sender</td>
<td>Shows a tabulated view of the top N devices that generated syslogs. The table shows the Syslog count by Severity.</td>
</tr>
<tr>
<td>Top N WAN Interface</td>
<td>Shows a tabulated view of the top N WAN Interfaces that reported issues along with the severity.</td>
</tr>
<tr>
<td>Syslog Summary</td>
<td>Shows syslogs of severity 0, 1 and 2.</td>
</tr>
<tr>
<td>Syslog Watch</td>
<td>The dashlet shows syslogs based on predefined filter, by default Environmental Monitor is selected.</td>
</tr>
</tbody>
</table>

Related Topics
- Adding Dashboards
- Restoring Dashboards
Time Filters for Dashboards and Dashlets

You can filter dashboards and dashlets based on a period of time. There are two ways to display information for a specified time:

- **By dashboard**—Using the Filters at the top of the Dashboard page, select a value from the Time Frame pulldown menu. Using the Filters feature allows you to filter all dashlet information for a specified time.
- **By dashlets**—Edit the dashlet to override a dashboard filter.

**Related Topic**
- **Overriding a Dashlet Filter**

Overriding a Dashlet Filter

You can change the filter settings for just one dashlet. For example, to change the time frame during which data is collected for a single dashlet from the default to 24 hours:

- **Step 1** Navigate to that dashlet and click Dashlet Options icon.
- **Step 2** Select the Override Dashboard Time Filter check box, choose Past 24 Hours from the Time Frame drop-down list, then click Save And Close.

The dashlet displays the last 24 hours of data, regardless of what is specified in the Dashboard Time Frame pulldown menu. The label “Edited” next to the Time Frame dashlet badge with a red diagonal line over the badge indicates that the filter has been customized.

**Related Topics**
- **Adding Dashboards**
- **Restoring Dashboards**

Creating Generic Dashlets

You can add a generic dashlet to the Performance dashboards and to any dashboard under the Performance tab. The generic dashlet displays the values for all polled devices.

**Before You Begin**

You must create at least one custom monitoring policy (for example, see Creating New Monitoring Policies).

To create a generic dashlet:

- **Step 1** Choose any dashboard under Dashboard > Performance.
- **Step 2** Click the Settings icon, then choose Add Dashlets.
- **Step 3** Find the Generic Dashlet and click Add. The Generic Dashlet appears on the dashboard.
- **Step 4** To edit the dashlet, hover your cursor over the Generic Dashlet and click Dashlet Options icon.
Chapter 10      Viewing and Managing Dashboards

Restoring Dashboards

After an upgrade, the arrangement of dashlets in the previous version is maintained. Therefore, dashlets or features added in a new release are not displayed. To display new dashlets, click the Settings icon and choose Manage Dashboards.

To restore a dashboard to the default settings:

Step 1  Click Settings at the top right of any dashboard page, then choose Manage Dashboards.
Step 2  Choose a dashboard from the list, and click Reset.

Related Topics
• Adding Dashboards
• Adding Dashlets
Troubleshooting Network Health Using Dashboards

Prime Infrastructure provides a quick way to view the health of your network and sites by choosing Dashboard > Network Summary > Network Health. You must create location groups and then add devices to the locations. Prime Infrastructure then displays a map indicating the overall health of all the sites. By default, all locations and a maximum of 500 APs per location group are displayed. You can use filters to modify the view.

Related Topics
- Defining Health Rules
- Network Health Map Features
- Network Health Summary
- Creating Location Groups

Defining Health Rules

You can specify rules and threshold values for your sites. The rules you specify determine the notifications that appear in Dashboard > Network Summary > Network Health.

Step 1
Choose Services > Application Visibility & Control > Health Rule. There are 3 tabs where you can specify health rules:
- Service Health—Define health rules for services such as jitter, MOS score, network time, packet loss, traffic rate, etc.
- Infrastructure Health—Define health rules for wired devices.
- Wireless Health—Define health rules for wireless devices.

Step 2
To add a new health rule, click the plus icon, then specify the location, metric, and threshold. You can add new Infrastructure Health and Wireless Health rules only.

Step 3
To edit an existing health rule, select the health rule you want to modify, then click Edit.

Step 4
Enter the details for the health rule, then click Save.
The values you enter apply to all devices and interfaces in the location group for which the health rule applies.
Network Health Map Features

When you choose Dashboard > Network Summary > Network Health, the map displays all the location groups with geographic attributes that you previously added. By default, a maximum of 500 APs per location group are displayed.

The location groups are colored according to the overall health of the location:

- Red—indicates there are critical issues in the specified location.
- Yellow—indicates there are warnings in the specified location.
- Green—indicates there are no errors or warnings.
- Gray—indicates there are no devices or data in the specified location.

In addition to the color indicating the health, the icon can be

- Solid—indicates a parent site, meaning there are children locations associated with the site.
- Outlined—indicates there are no children associated with this location.

Hover your mouse over any location on the map to view a popup window that lists the sites in that location and the corresponding errors or warnings, by device type, in each location.

Click on a site name to view in a zoomed-in map of the site.

Network Health Display Options

When you choose Dashboard > Network Summary > Network Health, display options appear on the right side of the page as show in Figure 11-1 and described in

Figure 11-1    Site Visibility Display Options
Related Topics

- Defining Health Rules
- Network Health Map Features
- Network Health Summary
- Creating Location Groups

**Network Health Summary**

The Health Summary pane displays errors and threshold violations for all devices across all locations. Prime Infrastructure aggregates health data from the devices and services to the site summary every 15 minutes. Click on any of the sites or devices listed in the Health Summary pane to view more information. For example, click on the site(s) listed under Service Health Issues. A new pane opens listing the sites with service health issues where you can easily see in which area(s) the errors or warnings are occurring.

Click on a site name to have the map zoom in on that particular site and display additional information specific to that site.

Related Topics

- Defining Health Rules
- Network Health Map Features
- Creating Location Groups
Monitoring Your Network

- Monitoring Devices
- Creating Monitoring Policies and Thresholds
- Monitoring Alarms
- Monitoring Clients and Users
- Configuring and Monitoring IWAN
- Monitoring Wireless Technologies
- Using Monitoring Tools
- Troubleshooting
- Monitoring Multiple Prime Infrastructure Instances
Monitoring Devices

The **Monitor > Managed Elements** menu provides tools to help you monitor your network on a daily basis, as well as perform other day-to-day or ad hoc operations relating to network device inventory and configuration management.

- Monitoring Network Devices
- Monitoring Jobs
- Monitoring Background Tasks
- Using Packet Capture to Monitor and Troubleshoot Network Traffic
- Securing Network Services

Monitoring Network Devices

Select **Monitor > Managed Elements > Network Devices** to view the list of devices that have been added to Prime Infrastructure. You can also add, edit, synchronize, and group devices.

**Related Topic**

- Network Devices Page
- Adding Devices Manually

Network Devices Page

Table 13-1 describes the information that is displayed when you select **Monitor > Managed Elements > Network Devices** to view the list of devices that have been added to Prime Infrastructure. You can sort the table by clicking on any cell heading.

<table>
<thead>
<tr>
<th>To View this Information</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device details such as software version, port information, CPU and memory utilization</td>
<td>Click on a Device Name.</td>
</tr>
<tr>
<td>Device 360 view</td>
<td>Click the icon in the IP Address field.</td>
</tr>
<tr>
<td>Collection status details</td>
<td>Click the icon in the Last Inventory Collection column.</td>
</tr>
</tbody>
</table>
Monitoring Jobs

Use the Jobs dashboard to:

- View all running and completed jobs and corresponding job details
- Filter jobs to view the specific jobs in which you are interested
- View details of the most recently submitted job
- View job execution results
- Modify jobs, including deleting, editing, running, canceling, pausing, and resuming jobs
- Change the refresh rate of the job dashboard
- Export job dashboard information in CSV or PDF formats

Prime Infrastructure can have a maximum of 25 jobs running concurrently. If a new job is created while 25 jobs are already running, the new job state is “scheduled” until a job completes and the new job can start. If a new job’s scheduled time has already passed before it could be started, the new job will not run and you’ll need to reschedule or start it when less than 25 jobs are running.

To monitor jobs, follow these steps:

**Step 1** Choose Administration > Dashboards > Job Dashboard.

**Step 2** Click a job, then perform any of the following actions:

- Click **Run** to start the currently scheduled job immediately. If a job has the status “failed,” click **Run** to resubmit the same job, which creates a new scheduled job with the same parameters as the previous job. Only the failed and partially successful devices within the job will be selected for retry.
- Click **Abort** to stop a discovery job currently in progress and return it to its scheduled state. You cannot abort all jobs. For example, you receive an error message if you try to abort a running configuration job.
- Click **Cancel** to delete any future scheduled jobs for the job you specified. If a job is currently running, it will complete.
- If you select any report status job listed under User Jobs, all the buttons will be disabled.

**Step 3** To change the auto refresh rate of the job dashboard, click **Settings**, then select a refresh rate. By default, the auto refresh rate is **Off**, and you must manually refresh the job dashboard by clicking the Refresh icon.

**Step 4** To view information on when the job was created, started or scheduled and its history, select a job to view the Job Detail View page. Hover the mouse over the **Status** column of the specific job to view the troubleshooting information for a failed job.

When a minute job is scheduled to run recursively, the first trigger of the job falls on n-th minute of the hour, as divided by the quartz scheduler, and successive runs will be placed as per the schedule. For example, if you have given the start time as 12:02:00 and you want the job to run every 3 minutes, then the job will be executed at 12:03 (in a minute), with the next recurrence at 12:06, 12:09, and so on.
Another example, if you have given the start time as 12:00:00 and you want the job to run every 3 minutes, then the job will be executed at 12:00 (without any delay), with the next recurrence at 12:03, 12:06, and so on.

Related Topic
- Viewing Options for Job Dashboard Metrics

Viewing Options for Job Dashboard Metrics

You can perform the following actions on the Metrics, which are displayed at the top of the Administration > Dashboards > Job Dashboard page:
- Add or remove metrics by selecting Settings > Add or Remove Metric Dashlet(s).
- Reorder the metrics by clicking near the metric title and dragging and dropping it to the area you prefer.
- Click any of the hyperlinks in any of the boxes to go to the details for that metric. When you click on a number in any of the boxes, the page filters and displays the jobs of the type you specified.

Monitoring Background Tasks

A background task is a scheduled program running in the background with no visible pages or other user interfaces. In Prime Infrastructure, background tasks can be anything from data collection to backing up configurations. You can monitor background tasks to see which background tasks are running, check their schedules, and find out whether the task was successfully completed.

To monitor the background tasks, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; Settings &gt; Background Tasks to view scheduled tasks. The Background Tasks page appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose a command from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>- Execute Now—Runs all of the data sets with a selected check box.</td>
</tr>
<tr>
<td></td>
<td>- Enable Tasks—Enables the data set to run on its scheduled interval.</td>
</tr>
<tr>
<td></td>
<td>- Disable Tasks—Prevents the data set from running on its scheduled interval.</td>
</tr>
</tbody>
</table>

Using Packet Capture to Monitor and Troubleshoot Network Traffic

In addition to aggregating data from multiple NAMs, Prime Infrastructure makes it easy to actively manage and troubleshoot network problems using multiple NAMs and ASRs.
This feature is supported for NAMs and ASRs. For more information on minimum Cisco IOS XE version supported on ASRs, see the Cisco ASR 1000 Series Aggregation Services Routers Release Notes.

In the following workflow, a network operator needs to troubleshoot a set of similar authentication violations taking place at multiple branches. Because the operator suspects that the authentication problems are due to a network attack in progress, the operator runs the Packet Capture feature against the NAMs or ASRs for each branch, then runs the Packet Decoder to inspect the suspicious traffic.

**Step 1** Create a capture session definition:

a. Choose **Monitor > Tools > Packet Capture**, then click **Capture Session** to create a new capture session definition.

b. Complete the **General** section as needed. Give the session definition a unique name and specify how you want to file the captured data. To capture the full packet, enter 0 in the Packet Slice Size.

c. If you want to restrict the captured traffic to particular source or destination IPs, VLANs, applications, or ports, click **Add** in the Software Filters section and create filters as needed. If you do not create a software filter, it captures everything.

d. In the **Devices** area, you can select:
   - A NAM and its data ports. You can create one capture session per NAM only, whether the capture session is running or not.
   - An ASR and its interfaces.

e. Click **Create and Start All Sessions**.

Prime Infrastructure saves the new session definition, then runs separate capture sessions on each of the devices you specified. It stores the sessions as files on the device and displays the list of packet capture files in the **Capture Files** area.

**Step 2** To decode a packet capture file:

a. Choose **Monitor > Tools > Packet Capture**.

b. Select a PCAP file in a NAM or ASR device.

c. Select **Copy To** to copy the PCAP file to the PI server (the decode operation only runs on files in the PI server).

d. Click **View Jobs** to confirm that the copy job completed successfully.

e. Open the localhost folder, select the check box for the new capture file, then click **Decode**. The decoded data appears in the bottom pane.

f. A TCP Stream displays the data as the application layer sees it. To view the TCP Stream for a decoded file, select a TCP packet from the Packet List, then click **TCP Stream**. You can view the data as ASCII text or in a HEX dump.

**Step 3** To run a packet capture session again, select the session definition in the **Capture Sessions** area and click **Start**.
Securing Network Services

Cisco TrustSec technology uses software-defined segmentation to simplify the provisioning of security policies, to accelerate security operations, and to consistently enforce policy anywhere in the network. TrustSec is embedded technology in Cisco switches, routers, wireless, and security devices. It is a secure network architecture that extends security across the network from campus to branch to data center. TrustSec is the foundation for using the Network as an Enforcer and mitigates risk by reducing attack surface through better segmentation, whilst also increasing operational efficiency and making compliance goals easier to achieve.
Monitoring Wireless Devices

You can monitor your wireless devices in your network on a daily basis, as well as perform other day-to-day or ad hoc operations related to wireless device inventory.

- Monitoring Controllers
- Monitoring Access Points
- Monitoring Rogue Access Points
- Monitoring Spectrum Experts
- Monitoring WiFi TDOA Receivers
- Monitoring Media Streams
- Monitoring Access Point Alarms

Monitoring Controllers

Choose Monitor > Managed Elements > Network Devices, then select Device Type > Wireless Controller to view all the wireless controllers.

Related Topic
- Monitoring System Parameters

Monitoring System Parameters

Choose Monitor > Managed Elements > Network Devices, then select Device Type > Wireless Controller to view all the wireless controllers. Click a Device name to view its details. You can monitor all the wireless controller details described in Table 14-1.
### Table 14-1  Monitor > Network Devices > Wireless Controller Details

<table>
<thead>
<tr>
<th>To View ...</th>
<th>Select This Menu ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Information</strong></td>
<td></td>
</tr>
<tr>
<td>Summary information such as IP address, device type, location, reachability status, description, etc.</td>
<td>System &gt; Summary under Device Details tab</td>
</tr>
<tr>
<td>CLI session details</td>
<td>System &gt; CLI Sessions under Device Details tab</td>
</tr>
<tr>
<td>DHCP statistics (for version 5.0.6.0 controllers or later) such as packets sent and received, DHCP server response information, and the last request time stamp</td>
<td>System &gt; DHCP Statistics under Device Details tab</td>
</tr>
<tr>
<td>Multicast information</td>
<td>System &gt; Multicast under Configuration tab</td>
</tr>
<tr>
<td>Stack information such as MAC address, role, state, etc.</td>
<td>System &gt; Stacks under Device Details tab</td>
</tr>
<tr>
<td>STP statistics</td>
<td>System &gt; Spanning Tree Protocol under Configuration tab</td>
</tr>
<tr>
<td>Information about any user-defined fields</td>
<td>System &gt; User Defined Field under Device Details tab</td>
</tr>
<tr>
<td>Wireless local access networks (WLANs) configured on a controller</td>
<td>System &gt; WLANs under Device Details tab</td>
</tr>
<tr>
<td><strong>Mobility</strong></td>
<td></td>
</tr>
<tr>
<td>Statistics for mobility group events such as receive and transmit errors, handoff request, etc.</td>
<td>Mobility &gt; Mobility Stats under Device Details tab</td>
</tr>
<tr>
<td><strong>Ports</strong></td>
<td></td>
</tr>
<tr>
<td>Information regarding physical ports on the selected controller</td>
<td>Ports &gt; General under Configuration tab</td>
</tr>
<tr>
<td>CDP Interfaces</td>
<td>Ports &gt; CDP Interface Neighbors under Configuration tab</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td></td>
</tr>
<tr>
<td>Information about location parameters such as expiration times, notification interval, etc.</td>
<td>Location &gt; Location Configuration under Configuration tab</td>
</tr>
<tr>
<td>Information about Global BLE Configuration on the controller.</td>
<td>Location &gt; Global BLE Configuration under Configuration tab</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
</tr>
<tr>
<td>RADIUS accounting server information and statistics</td>
<td>Security &gt; RADIUS Accounting under Device Details tab</td>
</tr>
<tr>
<td>RADIUS authentication server information</td>
<td>Security &gt; RADIUS Authentication under Device Details tab</td>
</tr>
<tr>
<td>Information about network access control lists</td>
<td>System &gt; Security &gt; Network Access Control</td>
</tr>
<tr>
<td>Guest access deployment and network users</td>
<td>Security &gt; Guest Users under Device Details tab</td>
</tr>
<tr>
<td>Management Frame Protection (MFP) summary information</td>
<td>System &gt; Security &gt; Management Frame Protection under Device Details tab</td>
</tr>
<tr>
<td>List of all rogue access point rules currently applied to a controller.</td>
<td>System &gt; Security &gt; Rogue AP Rules under Device Details tab</td>
</tr>
<tr>
<td>List of sleeping clients, which are clients with guest access that have had successful web authentication that are allowed to sleep and wake up without having to go through another authentication process through the login page</td>
<td>Security &gt; Sleeping Clients under Device Details tab</td>
</tr>
<tr>
<td><strong>IPv6</strong></td>
<td></td>
</tr>
</tbody>
</table>
Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a link management protocol. Cisco WLAN Solution implements the IEEE 802.1D standard for media access control bridges.

The spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

The following controllers do not support Spanning Tree Protocol: WISM, 2500, 5500, 7500 and SMWLC.

Related Topics

- Wireless Controller System Summary
- Spanning Tree Protocol
- Management Frame Protection
- Rogue AP Rules

Management Frame Protection

Management Frame Protection (MFP) provides the authentication of 802.11 management frames. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

If one or more of the WLANs for the controller has MFP enabled, the controller sends each registered access point a unique key for each BSSID the access point uses for those WLANs. Management frames sent by the access point over the MFP enabled WLANs is signed with a Frame Protection Information Element (IE). Any attempt to alter the frame invalidates the message causing the receiving access point configured to detect MFP frames to report the discrepancy to the WLAN controller.
Rogue AP Rules

Rogue AP rules automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. Prime Infrastructure applies the rogue access point classification rules to the controllers and respective access points.

These rules can limit a rogue appearance on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Rogue AP Rules also help reduce false alarms.

Rogue classes include the following types:

- Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
- Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
- Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

Related Topic
- Monitoring Controllers

Monitoring Third Party Controllers

Choose Monitor > Managed Elements > Network Devices > Third Party Wireless Controllers to view the detailed information about the third party (non-Cisco) controllers that are managed by Prime Infrastructure.

Monitoring Switches

Choose Monitor > Managed Elements > Network Devices > Switches and Hubs to view the following detailed information about the switches:

- Searching Switches
  Use the Prime Infrastructure search feature to find specific switches or to create and save custom searches.
- Viewing the Switches

Related topics
- Monitor > Switches > Search
- Monitor > Switches > View
Configuring the Switch List Page

The Edit View page allows you to add, remove, or reorder columns in the Switches table. To edit the available columns in the table, follow these steps:

**Step 1** Choose Monitor > Managed Elements > Network Devices > Switches and Hubs.

**Step 2** Click the Edit View link.

**Step 3** To add an additional column to the table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table.

**Step 4** To remove a column from the table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.

**Step 5** Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

**Step 6** Click Reset to restore the default view.

**Step 7** Click Submit to confirm the changes.

**Related topics**
- Monitor > Switches > Search
- Monitor > Switches > View

Monitoring Switch System Parameters

Choose Monitor > Managed Elements > Network Devices > Switches and Hubs, then click on a Device Name to view the following detailed information about the switch:

- Viewing Switch Memory Information
- Viewing Switch Environment Information
- Viewing Switch Module Information
- Viewing Switch VLAN Information
- Viewing Switch VTP Information
- Viewing Switch Physical Ports Information
- Viewing Switch Sensor Information
- Viewing Switch Spanning Tree Information
- Viewing Spanning Tree Details
- Viewing Switch Stacks Information
- Viewing Switch NMSP and Location Information

**Related Topics**
- Viewing Switch Information
Viewing Switch Information

To view switch information, follow these steps:

**Step 1** Choose Monitor > Managed Elements > Network Devices > Switches and Hubs.

**Step 2** Click an Device Name in the Device Name column to view details about the switch.

**Step 3** Click one of the following from the System menu to view the relevant information:
- Environment
- Modules
- VLANs
- VTP
- Physical Ports
- Sensors
- Spanning Tree
- Stacks
- NMSP and Location

Related Topic
- Monitoring Switch Interfaces
- Monitor > Switches > IP Address
- Monitor > Switches > Memory
- Monitor > Switches > Environment
- Monitor > Switches > Modules
- Monitor > Switches > VLANs
- Monitor > Switches > VTP
- Monitor > Switches > Physical Ports
- Monitor > Switches > Sensors
- Monitor > Switches > Spanning Tree
- Monitor > Switches > Spanning Tree Details
- Monitor > Switches > Stacks

Monitoring Switch Interfaces

**Step 1** Choose Monitor > Managed Elements > Network Devices > Switches and Hubs.

**Step 2** Click an Device Name in the Device Name column to view details about the switch.

**Step 3** Click Interfaces to view the following information:
- Monitoring Switch Ethernet Interfaces
- Monitoring Switch Ethernet Interface Details
Monitoring Switch IP Interfaces
Monitoring Switch VLAN Interfaces
Monitoring Switch EtherChannel Interfaces

Related Topics
- Viewing Switch Interface Information

Viewing Switch Interface Information

To view switch interface information, follow these steps:

**Step 1** Choose Monitor > Managed Elements > Network Devices > Switches and Hubs.
**Step 2** Click an Device Name in the Device Name column to view details about the switch.
**Step 3** Click Interfaces.
**Step 4** Click one of the following to view the relevant information:
- Ethernet Interfaces
- Ethernet Interface Name
- IP Interfaces
- VLAN Interfaces
- EtherChannel Interfaces

Related Topics
- Monitor > Switches > Interfaces > Ethernet Interfaces
- Monitor > Switches > Interfaces > Ethernet Interface Name
- Monitor > Switches > Interfaces > IP Interface
- Monitor > Switches > Interfaces > VLAN Interface
- Monitor > Switches > Interfaces > EtherChannel Interface

Monitoring Switch Clients

To view switch interface information, follow these steps:

**Step 1** Choose Monitor > Managed Elements > Network Devices > Switches and Hubs.
**Step 2** Click an Device Name in the Device Name column to view details about the switch.
**Step 3** Choose Clients from the System Menu to monitor switch clients.
Monitoring Access Points

This section describes access to the controller access points summary details. Use the main date area to access the respective access point details.

Choose Monitor > Wireless Technologies > Access Point Radios to access this page.

Related Topics
- Searching for Access Points
- Viewing a List of Access Points
- Types of Reports for Access Points
- Monitoring Access Points Details

Searching for Access Points

Use the Prime Infrastructure Search feature to find specific access points or to create and save custom searches.

Related Topics
- Viewing a List of Access Points
- Types of Reports for Access Points
- Monitoring Access Points
- Monitoring Access Points Details
- Search Methods

Viewing a List of Access Points

Choose Monitor > Wireless Technologies > Access Point Radios or perform an access point search to view the summary of access points including the default information.

Related Topics
- Searching for Access Points
- Types of Reports for Access Points
- Monitoring Access Points
- Monitoring Access Points Details
- Viewing a List of Access Points

Configuring the List of Access Points Display

The Edit View page allows you to add, remove, or reorder columns in the Access Points table.

To edit the available columns in the alarms table:

**Step 1** Choose Monitor > Wireless Technologies > Access Point Radios.
Step 2  Click the **Edit View** link.

Step 3  To add an additional column to the access points table, highlight the column heading in the left column and click **Show** to move the heading to the right column. An additional column will be added to the left of the highlighted column.

Step 4  To remove a column from the access points table, highlight the column heading of the column on the right of the column you want to remove and click **Hide**. All items in the left column will be removed from the table.

Step 5  Use the **Up/Down** buttons to specify the order in which the information appears in the table. Highlight the desired row heading and click **Up** or **Down** to move it higher or lower in the current list.

Step 6  Click **Reset** to restore the default view.

Step 7  Click **Submit** to confirm the changes.

---

**Related Topics**
- Monitoring Access Points
- Searching for Access Points
- Viewing a List of Access Points
- Monitoring Access Points Details

---

**Types of Reports for Access Points**

The following reports can be generated for Access Points. These reports cannot be customized.

- **Load**—Generates a report with load information.
- **Dynamic Power Control**—Generates a report with Dynamic Power Control information.
- **Noise**—Generates a report with Noise information.
- **Interference**—Generates a report with Interference information.
- **Coverage (RSSI)**—Generates a report with Coverage (RSSI) information.
- **Coverage (SNR)**—Generates a report with Coverage (SNR) information.
- **Up/Down Statistics**—Time in days, hours and minutes since the last reboot. Generates a report with Up Time information.
- **Network Airtime Fairness Statistics**—Tabular representation of Average Airtime used across different WLAN profiles in the selected interval of time.
- **Voice Statistics**—Generates a report for selected access points showing radio utilization by voice traffic.
- **Voice TSM Table**—Generates a report for selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.
- **Voice TSM Reports**—Graphical representation of the TSM table except that metrics from the clients are averaged together on the graphs.
- **802.11 Counters**—Displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.
- **AP Profile Status**—Displays access point load, noise, interference, and coverage profile status.
- Air Quality vs. Time—Displays the air quality index of the wireless network during the configured time duration.

- Traffic Stream Metrics—Determines the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.

- Tx Power and Channel—Displays the channel plan assignment and transmit power level trends of devices based on the filtering criteria used when the report was generated. It can help identify unexpected behavior or issues with network performance.

- VoIP Calls Graph—Helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. VoIP snooping must be enabled on the WLAN to be able to gather useful data from this report. This report displays information in a graph.

- VoIP Calls Table—Provides the same information as the VoIP Calls Graph report but in table form.

- Voice Statistics—Helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure call admission control (CAC) is supported on voice clients.

- Worst Air Quality APs—Provides a high-level, easy-to-understand metric to facilitate understanding of where interference problems are impacting the network. Air Quality (AQ) is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold.

**Related Topics**
- Monitoring Traffic Load
- Monitoring Dynamic Power Control
- Monitoring Access Points Noise
- Monitoring Access Points Interference
- Monitoring Access Points Coverage (RSSI)
- Monitoring Access Points Coverage (SNR)
- Monitoring Access Points Up/Down Statistics
- Monitoring the Access Points Voice Statistics
- Monitoring the Access Points Voice TSM Table
- Monitoring the Access Points Voice TSM Reports
- Monitoring Access Points 802.11 Counters
- Monitoring Access Points AP Profile Status
- Monitoring Air Quality
- Monitoring Access Points Traffic Stream Metrics
- Monitoring Access Points Tx Power and Channel
- Monitoring VoIP Calls
- Monitoring Voice Statistics
- Monitoring Air Quality
Generating Reports for Access Points

To generate a report for access points:

- **Step 1**: Choose **Monitor > Wireless Technologies > Access Point Radios**.
- **Step 2**: Click to select the access point(s) for which you want to run a report.
- **Step 3**: Choose the applicable report from the Select a report drop-down list.
- **Step 4**: Click **Go**.

**Related Topics**
- Types of Reports for Access Points

Monitoring Traffic Load

Traffic Load is the total amount of bandwidth used for transmitting and receiving traffic. This enables WLAN managers to track network growth and plan network growth ahead of client demand.

To generate the access point load report:

- **Step 1**: Choose **Monitor > Wireless Technologies > Access Point Radios**.
- **Step 2**: Select the check box(es) of the applicable access point(s).
- **Step 3**: From the Generate a report for selected APs drop-down list, choose **Load**.
- **Step 4**: Click **Go**. The Load report displays for the selected access points.

**Related Topics**
- Types of Reports for Access Points
- Monitor > Access Points > Load

Monitoring Dynamic Power Control

To generate the Access Point Load report:

- **Step 1**: Choose **Monitor > Wireless Technologies > Access Point Radios**.
- **Step 2**: Select the check box(es) of the applicable access point(s).
- **Step 3**: From the Generate a report for selected APs drop-down list, choose **Dynamic Power Control**.
- **Step 4**: Click **Go**. The Dynamic Power Control report displays the selected access points.

**Related Topics**
- Types of Reports for Access Points
- Monitor > Access Points > Dynamic Power Control
Monitoring Access Points Noise

To generate the Access Point Noise report:

Step 1  Choose Monitor > Wireless Technologies > Access Point Radios.
Step 2  Select the check box(es) of the applicable access point(s).
        If multiple access points are selected, they must have the same radio type.
Step 3  Choose Noise from the Generate a report selected APs drop-down list.
Step 4  Click Go.
        The Noise report displays a bar graph of noise (RSSI in dBm) for each channel for the selected access points.

Related Topics
•  Types of Reports for Access Points

Monitoring Access Points Interference

To generate the Access Point Interference report:

Step 1  Choose Monitor > Wireless Technologies > Access Point Radios.
Step 2  Select the check box(es) of the applicable access point(s).
        If multiple access points are selected, they must have the same radio type.
Step 3  Choose Interference from the Generate a report for selected APs drop-down list, then click Go.
        The Interference report displays a bar graph of interference (RSSI in dBm) for each channel:
        •  High interference -40 to 0 dBm.
        •  Marginal interference -100 to -40 dBm.
        •  Low interference -110 to -100 dBm.

Related Topics
•  Types of Reports for Access Points

Monitoring Access Points Coverage (RSSI)

To generate the Access Point Coverage (RSSI) report:

Step 1  Choose Monitor > Wireless Technologies > Access Point Radios
Step 2  Select the check box(es) of the applicable access point(s).
Step 3  Choose Coverage (RSSI) from the Generate a report for selected APs drop-down list.
Step 4 Click Go.

The Coverage (RSSI) report displays a bar graph of client distribution by received signal strength showing the number of clients versus RSSI in dBm.

Related Topics
- Types of Reports for Access Points

Monitoring Access Points Coverage (SNR)

To generate the Access Point Coverage (SNR) report:

Step 1 Choose Monitor > Wireless Technologies > Access Point Radios.
Step 2 Select the check box(es) of the applicable access point(s).
Step 3 Choose Coverage (SNR) from the Generate a report for selected APs drop-down list, then click Go.

The Access Points Coverage (SNR) report displays a bar graph of client distribution by signal-to-noise ratio showing the number of clients versus SNR.

Related Topics
- Types of Reports for Access Points

Monitoring Access Points Up/Down Statistics

To generate the Access Point Up/Down Statistics report:

Step 1 Choose Monitor > Wireless Technologies > Access Point Radios.
Step 2 Select the check box of the applicable access point.
Step 3 Choose Up/Down Statistics from the Generate a report for selected APs drop-down list. Click Go.

The Up/Down Statistics report displays a line graph of access point up time graphed against time.

Related Topics
- Types of Reports for Access Points

Monitoring the Access Points Voice Statistics

To generate the Access Point Voice Statistics report:

Step 1 Choose Monitor > Wireless Technologies > Access Point Radios.
Step 2  Select the check box(es) of the applicable access point(s).

Step 3  Choose **Voice Statistics** from the **Generate a report for selected APs** drop-down list, then click **Go**.

The Voice Statistics report displays the following radio utilization statistics by voice traffic:

- AP Name.
- Radio.
- Calls in Progress
- Roaming Calls in Progress
- Bandwidth in Use

Voice Statistics reports are only applicable for CAC/WMM clients.

---

**Related Topics**
- Types of Reports for Access Points

### Monitoring the Access Points Voice TSM Table

To access the Access Point Voice TSM Table report:

Step 1  Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2  Select the check box of the applicable access point.

Step 3  Choose **Voice TSM Table** from the **Generate a report for selected APs** drop-down list.

Step 4  Click **Go**.

The Voice Traffic Stream Metrics Table is generated for the selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.

---

**Related Topics**
- Types of Reports for Access Points
- **Monitor > Wireless Technologies > Access Point Radios > Voice TSM Table**

### Monitoring the Access Points Voice TSM Reports

To access the access point Voice Traffic Stream Metrics Table report:

Step 1  Choose **Monitor > Wireless Technologies > Access Point Radios**.

Step 2  Select the check box of the applicable access point.

Step 3  Choose **Voice TSM Reports** from the **Generate a report for selected APs** drop-down list.

Step 4  Click **Go**.
Chapter 14  Monitoring Wireless Devices

The Voice Traffic Stream Metrics Table report displays a graphical representation of the Voice Traffic Stream Metrics Table except that metrics from the clients that are averaged together on the graphs for the selected access point.

**Related Topics**
- Types of Reports for Access Points
- Monitor > Wireless Technologies > Access Point Radios > Voice TSM Reports

**Monitoring Access Points 802.11 Counters**

The 802.11 Counters report displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.

**Related Topics**
- Types of Reports for Access Points
- Generating Reports

**Monitoring Access Points AP Profile Status**

The AP Profile Status Report displays access point load, noise, interference, and coverage profile status.

**Related Topics**
- Types of Reports for Access Points
- Generating Reports

**Monitoring Access Points Radio Utilization**

The Radio Utilization Report displays the utilization trends of the access point radios based on the filtering criteria used when the report was generated. It helps to identify current network performance and capacity planning for future scalability needs.

**Related Topics**
- Types of Reports for Access Points
- Generating Reports

**Monitoring Access Points Traffic Stream Metrics**

The Traffic Stream Metrics Report is useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.
Related Topics
- Types of Reports for Access Points
- Generating Reports

Monitoring Access Points Tx Power and Channel

The Tx Power and Channel report displays the channel plan assignment and transmits power level trends of devices based on the filtering criteria used when the report was generated. It can help identify unexpected behavior or issues with network performance.

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the Product Guide or data sheet at for each specific model to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example. 2, 3, 4, and so on.) represents approximately a 50% (or 3dBm) reduction in transmit power from the previous power level. The actual power reduction might vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Irrespective of whether you choose Global or Custom assignment method, the actual conducted transmit power at the access point is verified such that country specific regulations are not exceeded.

The following command buttons are available to configure the transmission levels:
- Save—Save the current settings.
- Audit—Discover the present status of this access point.

Related Topics
- Types of Reports for Access Points
- Generating Reports

Monitoring VoIP Calls

VoIP Calls Report helps analyze wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. To be able to gather useful data from this report, VoIP snooping must be enabled on the WLAN. This report displays information in a graph.

Click VoIP Calls Graph from the Report Launch Pad to open the VoIP Calls Graph Reports page. From this page, you can enable, disable, delete, or run currently saved report templates.

Related Topics
- Types of Reports for Access Points
- Generating Reports
Monitoring Voice Statistics

Voice Statistics report helps analyze wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network.

To be able to gather useful data from this report, make sure Call Admission Control (CAC) is supported on voice clients.

Related Topics
- Types of Reports for Access Points
- Generating Reports

Monitoring Air Quality

To facilitate an easy understanding of where interference problems are impacting the network, Prime Infrastructure rolls up the detailed information into a high-level, easy-to-understand metric referred to as Air Quality (AQ). AQ is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold.

Related Topics
- Types of Reports for Access Points
- Generating Reports

Monitoring Access Points Details

The Access Points Details page enables you to view access point information for a single AP.

Choose Monitor > Wireless Technologies > Access Point Radios and click the access point name in the AP Name column to access this page. Depending on the type of access point, the following tabs are displayed:

- General Tab
  The General tab fields differ between lightweight and autonomous access points.
  For autonomous clients, Prime Infrastructure only collects client counts. The client counts in the Monitor page and reports have autonomous clients included. Client search, client traffic graphs, or other client reports (such as Unique Clients, Busiest Clients, Client Association) do not include clients from autonomous access points.

- Interfaces Tab

- CDP Neighbors Tab
  This tab is visible only when CDP is enabled.

- Current Associated Clients Tab
  This tab is visible only when there are clients associated to the AP (CAPWAP or Autonomous AP).

- SSID Tab
  This tab is visible only when the access point is an Autonomous AP and there are SSIDs configured on the AP.
- Clients Over Time Tab
  This tab displays the following charts:
  - Client Count on AP—Displays the total number of clients currently associated with an access point over time.
  - Client Traffic on AP—Displays the traffic generated by the client connected in the AP distribution over time.

  The information that appears in these charts is presented in a time-based graph. Time-based graphs have a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed.

**Related Topics**
- Types of Reports for Access Points
- Monitor > Wireless Technologies > Access Point Radios > General
- Monitor > Wireless Technologies > Access Point Radios > Interfaces
- Monitor > Wireless Technologies > Access Point Radios > CDP Neighbors
- Monitor > Wireless Technologies > Access Point Radios > Current Associated Clients
- Monitor > Wireless Technologies > Access Point Radios > SSID

### Monitoring Air Time Fairness

Cisco Air Time Fairness (ATF) for High Density Experience (HDX) allows network administrators to group devices of a defined category and enables some groups to receive traffic from the WLAN more frequently than other groups. Therefore, some groups are entitled to more air time than other groups.

Cisco ATF has the following capabilities:
- Allocates Wi-Fi air time for user groups or device categories
- Air time fairness is defined by the network administrator and not by the network
- Provides a simplified mechanism for allocating air time
- Dynamically adapts to changing conditions in a WLAN
- Enables a more efficient fulfillment of service-level agreements
- Augments standards-based Wi-Fi QoS mechanisms

**Related Topics**
- Monitoring ATF Statistics

### Monitoring ATF Statistics

1. **Step 1** Choose Monitor > Wireless Technologies > Access Point Radios.
2. **Step 2** Click the desired radio name in the Radio column.
   Depending on the type of access point, different tabs are displayed.
3. **Step 3** In the Access Point Radio Details, choose the Air Time Fairness tab.
The following charts are displayed:

- **Air Time Usage Absolute**—This chart represents the percent Air Time Usage by a WLAN on a Radio during the measured interval of time.
  - Click the calendar icon to choose the start date and year and end date and year or choose a preset value. The presets available are 1h, 6h, 1d, 1w, 2w, 4w, 3m, 6m, and 1y.
- **Air Time Usage Relative**—This chart displays the percent Air Time usage by a WLAN across all WLANs on a radio.
  - Click the calendar icon to choose the start date and year and end date and year or choose a preset value. The presets available are 1h, 6h, 1d, 1w, 2w, 4w, 3m, 6m, and 1y.

## Monitoring Rogue Access Points

A rogue device is an unknown access point or client that is detected by managed access points in your network. Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial of service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of clear-to-send (CTS) frames. This action mimics an access point informing a particular client to transmit and instructing all others to wait, which results in legitimate clients being unable to access network resources. Therefore, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Since rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad-hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security as they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having enterprise security breached.

### Related Topics

- Detecting Rogue Devices
- Classifying Rogue Access Points
- Monitoring Rogue AP Alarms
- Monitoring Ad hoc Rogues
- Searching Rogue Clients Using Advanced Search
- Monitoring Rogue Access Point Location, Tagging, and Containment

## Detecting Rogue Devices

Controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network. Prime Infrastructure consolidates all of the controllers rogue access point data.
You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue.

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, Prime Infrastructure uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

Related Topics
- Configuring Rogue Policies
- Monitoring Rogue Access Points
- Classifying Rogue Access Points
- Monitoring Rogue AP Alarms
- Monitoring Ad hoc Rogue Alarms

Classifying Rogue Access Points

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only. Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies whether the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.

5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.

6. The controller repeats the previous steps for all rogue access points.

7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.

8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state.

The following table shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

Table 14-2 Allowable Classification Type and Rogue State Transitions

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Friendly (Internal, External, Alert)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Friendly (Alert)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Malicious (Contained, Contained Pending)</td>
<td>Malicious (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert, Threat)</td>
<td>Friendly (Internal, External)</td>
</tr>
<tr>
<td>Unclassified (Contained, Contained Pending)</td>
<td>Unclassified (Alert)</td>
</tr>
<tr>
<td>Unclassified (Alert)</td>
<td>Malicious (Alert)</td>
</tr>
</tbody>
</table>

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

**Malicious Rogue APs**

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of Prime Infrastructure home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include:

- **Alert**—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly AP list.
- **Contained**—The unknown access point is contained.
Monitoring Rogue Access Points

- Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
- Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
- Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Only users can add a rogue access point MAC address to the Friendly AP list. Prime Infrastructure does not apply the Friendly AP MAC address to controllers.

The Security dashboard of Prime Infrastructure home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include the following:

- Internal—if the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
- External—if the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
- Alert—the unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points.

To delete a rogue access point from the Friendly AP list, ensure that both Prime Infrastructure and controller remove the rogue access point from the Friendly AP list. Change the rogue access point from Friendly AP Internal or External to Unclassified or Malicious Alert.

Unclassified Rogue APs

A rogue access point is called unclassified, if it is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the Prime Infrastructure home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include:

- Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- Alert—the unknown access point is not on the neighbor list or part of the user-configured Friendly AP list.
- Contained—the unknown access point is contained.
- Contained Pending—the unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information.
Related Topics
- Monitoring Rogue Access Points
- Detecting Rogue Devices

Monitoring Rogue AP Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco 1000 series lightweight access points. To open the Rogue AP Alarms page, do one of the following:
- Search for rogue APs.
- Navigate to Dashboard > Wireless > Security. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the AP number link in the Alarm Summary.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use it to view additional alarms.

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, Prime Infrastructure uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

When Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Viewing Rogue AP Alarm Details

Rogue access point radios are unauthorized access points detected by Cisco 1000 Series Lightweight APs. Alarm event details for each rogue access point are available in the Rogue AP Alarms list page.

To view alarm events for a rogue access point radio, select Monitor > Monitoring Tools > Alarms and Events, and click the arrow icon in a row to view Rogue AP Alarm Details page.

All Alarm Details page fields (except No. of Rogue Clients) are populated through polling and are updated every two hours. The number of rogue clients is a real-time number and is updated each time you access the Alarm Details page for a rogue access point alarm.

When a controller (version 7.4 or 7.5) sends custom rogue AP alarm, Prime Infrastructure shows it as unclassified rogue alarm. This is because Prime Infrastructure does not support custom rogue AP alarm.

When Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.
Viewing Rogue Client Details

You can view a list of rogue clients in several ways:

- Perform a search for rogue clients using Prime Infrastructure Search feature.
- View the list of rogue clients for a specific rogue access point from the Alarm Details page for the applicable rogue access point. Click the Rogue MAC address for the applicable rogue client to view the Rogue Client details page.
- In the Alarms Details page of a rogue access point, choose Rogue Clients from the Select a command drop-down list.

The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the associated rogue access point.

Rogue client statuses include: Contained (the controller contains the offending device so that its signals no longer interfere with authorized clients); Alert (the controller forwards an immediate alert to the system administrator for further action); and Threat (the rogue is a known threat). The higher the threat of the rogue access point, the higher the containment required.

Click the Client MAC Address for the rogue client to view the Rogue Client details page.

Related Topics

- Monitoring Rogue Access Points
- Monitoring Ad hoc Rogue Alarms
- Viewing Ad hoc Rogue Alarm Details
- Selecting Commands for Rogue AP Alarms

Viewing Rogue AP History Details

To view the history of a rogue AP alarms, click the Rogue AP History link in the Rogue AP Alarm page. Click the Rogue MAC address to view the specific rogue AP history details page.

Related Topics

- Rogue AP History Details Page
- Rogue AP Event History Details Page

Viewing Rogue AP Event History Details

To view the event details of a rogue AP, click the Event History link in the Rogue AP Alarm page.
Monitoring Ad hoc Rogues

If the MAC address of a mobile client operating in a ad hoc network is not in the authorized MAC address list, then it is identified as an ad hoc rogue.

Related Topics
- Viewing Rogue AP Alarm Details
- Viewing Rogue Client Details
- Viewing Rogue AP History Details
- Monitoring Ad hoc Rogue Alarms
- Viewing Ad hoc Rogue Alarm Details

Monitoring Ad hoc Rogue Alarms

The Adhoc Rogue Alarms page displays alarm events for ad hoc rogues. To access the Adhoc Rogue Alarms page, do one of the following:
- Perform a search for ad hoc rogue alarms.
- Navigate to Dashboard > Wireless > Security. This page displays all the ad hoc rogues detected in the past hour and the past 24 hours. Click the ad hoc rogue number to view the ad hoc rogue alarms.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

When Prime Infrastructure polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Related Topics
- Viewing Rogue AP History Details
- Viewing Ad hoc Rogue Alarm Details
- Selecting Commands for Rogue AP Alarms

Viewing Ad hoc Rogue Alarm Details

Alarm event details for each ad hoc rogue is available on the Adhoc Rogue Alarms page. Rogue access point radios are unauthorized access points detected by Cisco 1000 Series Lightweight APs.
To view alarm events for an ad hoc rogue radio, click the applicable Rogue MAC address in the Adhoc Rogue Alarms page.

When Prime Infrastructure polls, some data might change or get updated. Hence some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Alarms will not be triggered if a rogue is discovered using switch port tracing as switch port tracing does not update any of the rogue attributes such as severity, state, and so on.

Related Topics
- Searching Rogue Clients Using Advanced Search
- Viewing Ad hoc Rogue Alarm Details
- Selecting Commands for Rogue AP Alarms

Searching Rogue Clients Using Advanced Search

When the access points on your WLAN are powered up and associated with controllers, Prime Infrastructure immediately starts listening for rogue access points. When a controller detects a rogue access point, it immediately notifies Prime Infrastructure, which creates a rogue access point alarm.

To find rogue access point alarms using Advanced Search, follow these steps:

**Step 1** Click **Advanced Search** in the top right-hand corner of the Prime Infrastructure main page.

**Step 2** Choose **Rogue Client** from the Search Category drop-down list.

You can filter the search even further with the other search criteria if desired.

**Step 3** Click **Search**. The list of rogue clients appears.

**Step 4** Choose a rogue client by clicking a client MAC address. The Rogue Client detail page appears.

**Step 5** To modify the alarm, choose one of these commands from the **Select a Command** drop-down list, and click **Go**.

- **Set State to ‘Unknown-Alert’**—Tags the ad hoc rogue as the lowest threat, continues to monitor the ad hoc rogue, and turns off containment.
- **1 AP Containment through 4 AP Containment**—Indicates the number of access points (1-4) in the vicinity of the rogue unit that send deauthenticate and disassociate messages to the client devices that are associated to the rogue unit.
- **Map (High Resolution)**—Displays the current calculated rogue location in the Maps > Building Name > Floor Name page.
- **Location History**—Displays the history of the rogue client location based on RF fingerprinting. The client must be detected by an MSE for the location history to appear.

Related Topics
- Viewing Rogue AP Alarm Details
- Monitoring Rogue Access Point Location, Tagging, and Containment
Monitoring Rogue Access Point Location, Tagging, and Containment

Prime Infrastructure generates the flags as rogue access point traps and displays the known rogue access points by MAC address Cisco Unified Network Solution is monitoring it.

The operator displays a map showing the location of the access points closest to each rogue access point. These access points are classified as:

- Known or Acknowledged rogue access points (no further action)
- Alert rogue access points (watch for and notify when active)
- Contained rogue access points

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points.
- Receive new rogue access point notifications, eliminating hallway scans.
- Monitor unknown rogue access points until they are eliminated or acknowledged.
- Determine the closest authorized access point, making directed scans faster and more effective.
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or WLAN security
  - Accept rogue access points when they do not compromise the LAN or WLAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
- Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Related Topics

- Detecting Access Points
- Monitoring Rogue Alarm Events

Detecting Access Points

Use the Detecting Access Points feature to view information about the Cisco Lightweight APs that are detecting a rogue access point.

To access the Rogue AP Alarms details page, follow these steps:

**Step 1** To display the Rogue AP Alarms page, do one of the following:

- Perform a search for rogue APs.
- Navigate to Dashboard > Wireless > Security. This dashboard displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
Monitoring Ad hoc Rogues

Step 2
In the Rogue AP Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue AP Alarms details page appears.

Step 3
From the Select a command drop-down list, choose Detecting APs.

Step 4
Click Go.

Click a list item to display data about that item.

Related Topics
- Monitoring Rogue Access Point Location, Tagging, and Containment
- Monitoring Rogue Alarm Events

Monitoring Rogue Alarm Events

The Events page enables you to review information about rogue alarm events. Prime Infrastructure generates an event when a rogue access point is detected or if you make manual changes to a rogue access point (such as changing its state). The Rogue AP Events list page displays all rogue access point events.

To access the Rogue AP Events list page, follow these steps:

Step 1
Do one of the following:
- Perform a search for rogue access point events using the Advanced Search feature of Prime Infrastructure.
- In the Rogue AP Alarms details page, click Event History link.

Related Topics
- Detecting Access Points
- Viewing Rogue AP Event Details
- Rogue AP Event History Details Page

Viewing Rogue AP Event Details

To view rogue access point event details, in the Rogue AP Events list page, click the Rogue MAC Address link.

Related Topics
- Monitoring Rogue Alarm Events
- Monitoring Ad hoc Rogue Events
- Rogue AP Event History Details Page
- Selecting Commands for Rogue AP Alarms
Monitoring Ad hoc Rogue Events

The Events page enables you to review information about ad hoc rogue events. Prime Infrastructure generates an event when an ad hoc rogue is detected or if you make manual changes to an ad hoc rogue (such as changing its state). The Adhoc Rogue Events list page displays all ad hoc rogue events.

To access the Rogue AP Events list page, either perform a search for ad hoc rogues events using the Advanced Search feature of Prime Infrastructure or in the Adhoc Rogue Alarms details page, click Event History from the Select a Command drop-down list.

Related Topics
- Viewing Rogue AP Event Details
- Viewing Ad hoc Rogue Event Details

Viewing Ad hoc Rogue Event Details

To view rogue access point event details, in the Rogue AP Events list page, click the Rogue MAC Address link.

Related Topics
- Viewing Rogue AP Event Details
- Monitoring Ad hoc Rogue Events
- Rogue AP Event History Details Page

Troubleshooting Unjoined Access Points

When a lightweight access point initially starts up, it attempts to discover and join a WLAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all the configuration details for the device and network. After successfully joining the wireless controller, the access point can be discovered and managed by Prime Infrastructure. Until the access point successfully joins a wireless controller the access point cannot be managed by Prime Infrastructure and does not contain the proper configuration settings to allow client access.

Prime Infrastructure provides you with a tool that diagnoses why an access point cannot join a controller and lists corrective actions.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included in the page. This includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason if known.

To troubleshoot unjoined access points, do the following:

Step 1 Choose Monitor > Wireless Technologies > Unjoined Access Points. The Unjoined APs page appears containing a list of access points that have not been able to join a wireless controller.

Step 2 Select the access point that you wish to diagnose, then click Troubleshoot.
An analysis is run on the access point to determine the reason why the access point was not able to join a wireless controller. After performing the analysis, the Unjoined APs page displays the results. The middle pane, you can view what the problem is. It will also list error messages and controller log information.

**Step 3** Select a controller.

If the access point has tried to join multiple wireless controllers and has been unsuccessful, the controllers are listed in the left pane.

**Step 4** Perform one of the recommended actions from the list of recommendations for solving the problems listed in the right pane.

**Step 5** Run RTTS through the Unjoined AP page to further diagnose a problem. This allows you to see the debug messages from all the wireless controllers that the access point tried to join at one time.

To run RTTS, click the RTTS icon ( ) located to the right of the table. The debug messages appear in the table. You can then examine the messages to see if you can determine a cause for the access point not being able to join the controllers.

---

**Related Topics**
- Monitoring Rogue Access Points
- Monitoring Ad hoc Rogues

---

**Monitoring Spectrum Experts**

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to Prime Infrastructure. This feature allows Prime Infrastructure to collect, archive and monitor detailed interferer and air quality data from Spectrum Experts in the network.

To access the Monitor Spectrum Experts page, follow these steps:

**Step 1** Choose Services > Mobility Services > Spectrum Experts.

From the left sidebar menu, you can access the Spectrum Experts Summary page.

---

**Related Topics**
- Field Reference guide for Spectrum Experts Summary
- Field Reference guide for Interferer’s Summary
- Field Reference guide for Spectrum Experts Details
- Searching Interferers

---

**Monitoring WiFi TDOA Receivers**

The WiFi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset.
To view WiFi TDOA receiver information:

**Step 1** Choose Monitor > Wireless Technologies > WiFi TDOA Receivers.

Related Topics
- Searching WiFi TDOA Receivers

### Searching WiFi TDOA Receivers

To refine the search criteria for WiFi TDOA receivers:

**Step 1** Click the Advanced Search in the Prime Infrastructure user interface.

**Step 2** Choose WiFi TDOA Receiver from the Search Category drop-down list.
- To initiate a search for a Wi-Fi TDOA receiver by its MAC address, choose MAC Address from the Search drop-down list and enter the MAC address of the Wi-Fi TDOA receiver in the available text box, and click Search.
- To initiate a search for a Wi-Fi TDOA receiver by its name, choose WiFi TDOA Receivers from the Search by drop-down list and enter the name of the Wi-Fi TDOA receiver in the available text box, and click Search.

Related Topics
- Monitoring WiFi TDOA Receivers

### Monitoring Media Streams

To view all the media streams configured across controllers:

**Step 1** Choose Monitor > Wireless Technologies > Media Streams.

Related Topics
- Viewing Media Stream Details

### Viewing Media Stream Details

To view media stream details:

**Step 1** Choose Monitor > Wireless Technologies > Media Streams.
Radio Resource Management

The Radio Resource Management (RRM), built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment. Prime Infrastructure receives traps whenever a change in the transmit power in the access point or channel occurred. These trap events or similar events such as RF regrouping are logged into Prime Infrastructure and are maintained by the event dispatcher.

RRM automatically detects and configures new controllers and lightweight access points as they are added to the network. It automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity. Lightweight access points can simultaneously scan all valid 802.11b/g channels for the country of operation as well as for channels available in other locations. The access points go off-channel for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

The following notifications are sent to RRM dashboard:

- Channel change notifications are sent when a channel change occurs. Channel change depends on the Dynamic Channel Assignment (DCA) configuration.
- Transmission power change notifications are sent when transmission power changes occur. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- RF grouping notifications are sent when there is a RF grouping content change and automatic grouping is enabled.

Viewing the RRM Dashboard

To view the RRM dashboard information:


Related Topics
- Radio Resource Management
Monitoring Access Point Alarms

To monitor the Access Point (AP) alarms on your network:

**Step 1** Perform an advanced search for AP alarms.

The Search Results page contains the following information for AP alarms. You can select the check box next to the alarm and modify the required fields in the Alarm Browser toolbar.

- Severity
- Failure Source
- Owner
- Time
- Message
- Category
- Condition
- Acknowledged

**Step 2** Select the check box next to the alarm and modify the required fields in the Alarm Browser toolbar.

Monitoring Air Quality Alarms

To monitor air quality alarms on your network:

**Step 1** Perform an advanced search for Performance alarms.

The Search Results page contains the following information for air quality alarms.

- Severity
- Failure Source
- Owner
- Time
- Message
- Category
- Condition
- Acknowledged

**Step 2** Select the check box next to the alarm and modify the required fields in the Alarm Browser toolbar.

Monitoring CleanAir Security Alarms

To monitor CleanAir security alarms:
Step 1 Perform an advanced search for **Security** alarms.

The **Search Results** page contains the following information for CleanAir Security alarms.

- Severity
- Failure Source
- Owner
- Date/Time
- Message
- Acknowledged

Step 2 Select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

---

**Monitoring Cisco Adaptive wIPS Alarms**

Alarms from Cisco Adaptive wIPS DoS (denial of service) and security penetration attacks are classified as security alarms.

To view a list of wIPS DoS and security penetration attack alarms:

Step 1 Perform an advanced search for **wIPS DoS** alarms.

The **Search Results** page contains the following information.

- Severity
- Failure Object
- Date/Time
- Message
- Acknowledged
- Category
- Condition
- When there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

Step 2 Select the check box next to the alarm and modify the required fields in the **Alarm Browser** toolbar.

---

**Monitoring Cisco Adaptive wIPS Alarm Details**

To monitor Cisco Adaptive wIPS alarm details:

Choose **Monitor > Monitoring Tools > Alarms and Events > failure object** to view details of the selected Cisco wIPS alarm. The following Alarm details are provided for Cisco Adaptive wIPS alarms:

- General
  - Detected By wIPS AP—The access point that detected the alarm.
- wIPS AP IP Address—The IP address of the wIPS access point.
- Owner—Name of person to which this alarm is assigned or left blank.
- Acknowledged—Displays whether or not the alarm is acknowledged by the user.
- Category—For wIPS, the alarm category is Security.
- Created—Month, day, year, hour, minute, second, AM or PM that the alarm was created.
- Modified—Month, day, year, hour, minute, second, AM or PM that the alarm was last modified.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events.
  - Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them.
- Severity—Level of severity including critical, major, info, warning, and clear.
- Last Disappeared—The date and time that the potential attack last disappeared.
- Channel—The channel on which the potential attack occurred.
- Attacker Client/AP MAC—The MAC address of the client or access point that initiated the attack.
- Attacker Client/AP IP Address—The IP address of the client or access point that initiated the attack.
- Target Client/AP IP Address—The IP address of the client or access point targeted by the attacker.
- Controller IP Address—The IP address of the controller to which the access point is associated.
- MSE—The IP address of the associated mobility services engine.
- Controller MAC address—The MAC address of the controller to which the access point is associated.
- wIPS access point MAC address
- Forensic File
- Event History—Takes you to the Monitoring Alarms page to view all events for this alarm.

- Annotations—Displays any annotations that you have entered.
- Messages—Displays information about the alarm.
- Audit Report—Click to view configuration audit alarms details. This report is only available for Configuration Audit alarms.
  - Configuration audit alarms are generated when audit discrepancies are enforced on configuration groups.
- Rogue Clients—If the failure object is a rogue access point, information about rogue clients is displayed.

Related Topics
- Monitoring Cisco Adaptive wIPS Alarms
Monitoring Failure Objects

To monitor failure objects, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Alarms and Events, then click the Events tab.

**Step 2** Click the expand icon to the left of the Description column. Depending on the type of event you selected, the associated details vary.

- **General Info**
  - Failure Source—Indicates the source of the event (including name and/or MAC address).
  - Category—Type of alarm such as Security or AP.
  - Generated—Date and time that the event was generated.
  - Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
    - NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events.
    - Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them.
  - Device IP Address—IP address of the alarm-generating device.
  - Severity—Level of severity including critical, major, info, warning, and clear.
- **Messages**—Message explaining why the event occurred.

Monitoring Events for Rogue Access Points

To monitor events for rogue access points:

**Step 1** Choose Monitor > Monitoring Tools > Alarms and Events, then click the Events tab.

**Step 2** Use the Quick Filter or Advanced Filter feature to monitor the Rogue APs.

**Step 3** Click the expand icon to view alarm events for a rogue access point radio.

The following fields appear:

**General**

- Rogue MAC Address
- Vendor
- On Network—Indicates how the rogue detection occurred.
  - Controller—The controller detected the rogue (Yes or No).
  - Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.
- Owner—Name of person to which this alarm is assigned, or (blank).
• State—State of this radio relative to the network or Port. Rogue access point radios appear as “Alert” when first scanned by the Port, or as “Pending” when operating system identification is still underway.

• SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)

• Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.

• Channel—Indicates the band at which the ad hoc rogue is broadcasting.

• Radio Type—Lists all radio types applicable to this rogue access point.

• Created—Date and time that the event occurred.

• Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  – NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events.
  – Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them.

• Device IP Address—IP address of the alarm-generating device.

• Severity—Level of severity, Critical, Major, Minor, Warning, and Clear, Info.

Message—Displays descriptive information about the alarm.

Help—Displays information about the alarm.

Related Topics
• Monitoring Rogue Access Points

Monitoring Events for Ad hoc Rogues

To monitor events for ad hoc rogues:

Step 1 Choose Monitor > Monitoring Tools > Alarms and Events, then click the Events tab.

Step 2 Use the Quick Filter or Advanced Filter feature to monitor the events for Ad hoc Rogue APs.

Step 3 Click the expand icon to view alarm events for an ad hoc rogue access point. The following fields are displayed:

General
• Rogue MAC Address
• Vendor
• On Network—Indicates how the rogue detection occurred.
Chapter 14  Monitoring Wireless Devices

Monitoring Access Point Alarms

- Controller—The controller detected the rogue (Yes or No).
- Switch Port Trace—The rogue was detected by a switch port trace. Indicated by one of the following: Traced but not found, Traced and found, Not traced.

- Owner—Name of person to which this alarm is assigned, or (blank).
- State—State of this radio relative to the network or Port. Rogue access point radios appear as “Alert” when first scanned by the Port, or as “Pending” when operating system identification is still underway.
- SSID—Service Set Identifier being broadcast by the rogue access point radio. (Blank if SSID is not broadcast.)
- Containment Level—An access point which is being contained is either unable to provide service at all, or provides exceedingly slow service. There is a level associated with the containment activity which indicates how many Cisco 1000 series lightweight access points to use in containing the threat. This service must be initiated and halted by the administrator. Containment Type - Contained if the rogue access point clients have been contained at Level 1 through Level 4 under Update Status, otherwise Unassigned.
- Channel—Indicates the band at which the ad hoc rogue is broadcasting.
- Created—Date and time that the event occurred.
- Generated By—Indicates how the alarm event was generated (either NMS or from a trap).
  - NMS (Network Management System - Prime Infrastructure)—Generated through polling. Prime Infrastructure periodically polls the controllers and generates events. Prime Infrastructure generates events when the traps are disabled or when the traps are lost for those events.
  - Trap—Generated by the controller. Prime Infrastructure process these traps and raises corresponding events for them.
  - Device IP Address—IP address of the alarm-generating device.

Message—Displays descriptive information about the alarm.

Step 4  Help—Displays information about the alarm.

Related Topics
- Monitoring Rogue Access Points

Monitoring Cisco Adaptive wIPS Events

To monitor Cisco adaptive wIPS events:

Step 1  Choose Monitor > Monitoring Tools > Alarms and Events, then click the Events tab.
Step 2  Use the Quick Filter or Advanced Filter feature to narrow down the search results to monitor wIPS events. One or more events might generate an abnormal state or alarm. The alarm can be cleared, but the event remains.
Monitoring CleanAir Air Quality Events

To view the events generated on CleanAir air quality of the wireless network:

**Step 1**
Perform an advanced search for **Performance** event.

The **Search Results** page contains the following CleanAir air quality events information:

- **Severity**—Indicates the severity of the alarm.
- **Failure Source**—Device that generated the alarm.
- **Date/Time**—The time at which the alarm was generated.

**Related Topics**
- [Viewing Air Quality Event Details](#)

**Viewing Air Quality Event Details**

To view air quality event details:

**Step 1**
From the Air Quality Events page, click an expand icon adjacent to **Severity** column to access the alarm details page.

**Step 2**
The air quality event page displays the following information:

- **Failure Source**—Device that generated the alarm.
- **Category**—The category this event comes under. In this case, Performance.
- **Created**—The time stamp at which the event was generated.
- **Generated by**—The device that generated the event.
- **Device IP Address**—The IP address of the device that generated the event.
- **Severity**—The severity of the event.
- **Alarm Details**—A link to the related alarms associated with this event. Click the link to learn more about the alarm details.
- **Message**—Describes the air quality index on this access point.

Monitoring Interferer Security Risk Events

To monitor interferer security risk events:

**Step 1**
To view the security risk event generated on your wireless network, perform an advanced search for **Security** event.

The **Search Results** page contains the following interferer security events information:

- **Severity**—Indicates the severity of the alarm.
- **Failure Source**—Device that generated the alarm.
• Date/Time—The time at which the alarm was generated.

Related Topics
• Viewing Interferer Security Risk Event Details

Viewing Interferer Security Risk Event Details

To view interferer security event details:

Step 1
In the Interferer Security Event details page, click an expand icon adjacent to Severity column to access the alarm details page.

Step 2
The air quality event page displays the following information:
• Failure Source—Device that generated the alarm.
• Category—The category this event comes under. In this case, Security.
• Created—The time stamp at which the event was generated.
• Generated by—The device that generated the event.
• Device IP Address—The IP address of the device that generated the event.
• Severity—The severity of the event.
• Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
• Message—Describes the interferer device affecting the access point.

Related Topics
• Monitoring Interferer Security Risk Events

Monitoring Health Monitor Events

To view the health monitor events:

Step 1
Perform an advanced search for Prime Infrastructure event.

The Search Results page contains the following health monitor events related information:
• Severity—Indicates the severity of the alarm.
• Failure Source—Device that generated the alarm.
• Date/Time—The time at which the alarm was generated.
• Message—Describes the health details.

Related Topics
• Viewing Health Monitor Event Details
Viewing Health Monitor Event Details

To view health monitor event details:

**Step 1**
In the Health Monitor Events page, click an expand icon adjacent to **Severity** column to access the alarm details page.

**Step 2**
The Health Monitor Events page displays the following information:

- Failure Source—Device that generated the alarm.
- Category—The category this event comes under.
- Created—The time stamp at which the event was generated.
- Generated by—The device that generated the event.
- Device IP Address—The IP address of the device that generated the event.
- Severity—The severity of the event.
- Alarm Details—A link to the related alarms associated with this event. Click the link to know more about the alarm details.
- Message—Describes the event through a message.

**Related Topics**

- Monitoring Health Monitor Events
Creating Monitoring Policies and Thresholds

Prime Infrastructure uses monitoring policies to monitor devices against the thresholds you specify. When the thresholds that you specify are reached, Prime Infrastructure issues an alarm. The alarms warn you of changing conditions before the issues impact operations.

By default, Prime Infrastructure polls:

- Device health metrics on supported routers, switches and hubs. Storage devices and UCS series devices are not monitored by the default health policy. See Modifying Default Monitoring Policies.
- Port group health metrics.
- Interface health metrics on WAN interface groups, AVC, LISP, UCS and Nexus-VPC.

**Note** Prime Infrastructure uses monitoring policies only for Wired devices.

You can also enable other Prime Infrastructure monitoring policies or create a custom MIB polling policy (see Monitoring Third-Party Devices By Polling MIBs).

### Default Monitoring Policies

Prime Infrastructure polls SNMP objects to gather monitoring information for the following health monitoring policies under **Monitor > Monitoring Tools > Monitoring Policies > Automonitoring**:

- Device Parameters—Table 15-1 describes the device health parameters that are polled.
- Interface Parameters—Table 15-2 describes the interface parameters that are polled for:
  - Trunk and Link Ports
  - WAN Interfaces

For the following monitoring policies that provide assurance information, data is collected through NetFlow or NAMs:

- Application Response Time
- NAM Health
- Traffic Analysis
- Voice Video Data
- Voice Video Signaling
Table 15-1  *Device Parameter Automonitoring Metrics*

<table>
<thead>
<tr>
<th>Metric</th>
<th>Devices Polled</th>
<th>MIB</th>
<th>MIB Objects Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Availability</td>
<td>All SNMP devices</td>
<td>SNMPv2-MIB</td>
<td>sysUpTime</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Cisco IOS devices, All Supported Nexus devices, Cisco UCS devices</td>
<td>CISCO-PROCESS-MIB</td>
<td>cpmCPUPTotalPhysicalIndex cpmCPUPTotal1minRev</td>
</tr>
<tr>
<td>Memory Pool Utilization</td>
<td>Cisco IOS devices, ISR devices.</td>
<td>CISCO-MEMORY-POOL-MIB</td>
<td>ciscoMemoryPoolName ciscoMemoryPoolType ciscoMemoryPoolUsed ciscoMemoryPoolFree</td>
</tr>
<tr>
<td></td>
<td>All supported Cisco Nexus devices, Cisco UCS devices and Cisco IOS XE devices</td>
<td>CISCO-PROCESS-MIB</td>
<td>cpmCPUPTotalIndex cpmCPUMemoryUsed cpmCPUMemoryFree</td>
</tr>
<tr>
<td></td>
<td>Cisco ASA devices, IOS XR and Edison devices</td>
<td>CISCO-ENHANCED-MEMPOOL-MIB</td>
<td>cempMemPoolType cempMemPoolName cempMemPoolUsed cempMemPoolFree</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS ASR devices</td>
<td>CISCO-ENTITY-QFP-MIB</td>
<td>ceqfpMemoryResType ceqfpMemoryResInUse ceqfpMemoryResFree</td>
</tr>
<tr>
<td>Environment Temp</td>
<td>ASR, All Supported Nexus devices, Cisco UCS devices</td>
<td>CISCO-ENVMON-MIB</td>
<td>entSensorValue</td>
</tr>
<tr>
<td></td>
<td>Catalyst 2000, 3000, 4000, 6000, ISR</td>
<td>CISCO-ENVMON-MIB</td>
<td>ciscoEnvMonTemperatureStatusValue</td>
</tr>
</tbody>
</table>

1. For stacked switch devices, the Environment Temp displays the temperature of each stacked instance.
### Table 15-2  Interface Parameter Automonitoring Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Devices Polled</th>
<th>MIB</th>
<th>MIB Objects Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Availability</td>
<td>Cisco IOS devices, All Supported Nexus devices</td>
<td>IF-MIB</td>
<td>ifOperStatus, ifOutOctets, ifHighSpeed, ifInOctets, ifInErrors, ifOutErrors, ifInDiscards, ifOutDiscards</td>
</tr>
<tr>
<td>Input Utilization</td>
<td>Cisco IOS devices</td>
<td>IF-MIB, Old-CISCO-Interface-MIB</td>
<td>ifHCInBroadcastPkts, ifHCInMulticastPkts, ifInErrors, ifInDiscards, ifInUnknownProtos, ifHCInBroadCastPkts, ifHCInMulticastPkts</td>
</tr>
<tr>
<td>Output Utilization</td>
<td>Cisco IOS devices</td>
<td>IF-MIB, Old-CISCO-Interface-MIB</td>
<td>ifHCInBroadcastPkts, ifHCInMulticastPkts, ifHCInUcastPkts, ifInDiscards, ifInUnknownProtos, locIfInputQueueDrops</td>
</tr>
<tr>
<td>Percent Drop per QoS Class</td>
<td>Cisco IOS devices</td>
<td>IF-MIB, Old-CISCO-Interface-MIB</td>
<td>ifHCOutBroadcastPkts, ifHCOutMulticastPkts, ifHCOutUcastPkts, ifOutDiscards, ifOutUnknownProtos, locIfOutputQueueDrops</td>
</tr>
</tbody>
</table>

### Table 15-3  Class-Based, QoS, Health-Monitoring Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Devices Polled</th>
<th>MIB</th>
<th>MIB Objects Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>QOS calculation</td>
<td>Cisco IOS devices</td>
<td>CISCO-CLASS-BASED-QOS-MIB</td>
<td>cbQosCMDropByte64, cbQosCMPPostPolicyByte64, cbQosCMPrePolicyByte64</td>
</tr>
<tr>
<td>Interface Inbound Errors</td>
<td>Cisco IOS devices</td>
<td>IF-MIB</td>
<td>ifInErrors</td>
</tr>
<tr>
<td>Interface Outbound Errors</td>
<td>Cisco IOS devices</td>
<td>IF-MIB</td>
<td>ifOutErrors</td>
</tr>
<tr>
<td>Interface Inbound Discards</td>
<td>Cisco IOS devices</td>
<td>IF-MIB</td>
<td>ifInDiscards</td>
</tr>
<tr>
<td>Interface Outbound Discards</td>
<td>Cisco IOS devices</td>
<td>IF-MIB</td>
<td>ifOutDiscards</td>
</tr>
</tbody>
</table>
Modifying Default Monitoring Policies

Prime Infrastructure monitoring policies monitor network device metrics and alert you of changing conditions before the issues impact their operation. By default, Prime Infrastructure polls device health metrics on supported routers, switches and hubs only, and interface health metrics on WAN interfaces, links, and trunk ports. It is not polled on storage devices, and UCS series devices. If a threshold is violated three times, Prime Infrastructure generates a critical alarm, which is displayed on the Monitor > Monitoring Tools > Alarms and Events page.

To modify or disable the polling frequency and the threshold parameters, follow these steps:

---

**Step 1** Choose Monitor > Monitoring Tools > Monitoring Policies > Automonitoring.

**Step 2** Select Device Health, then modify the polling frequencies and thresholds as desired.

**Step 3** Click:
- **Save and Activate** to save and activate the policy immediately on the selected devices.
- **Save and Close** to save the policy and activate it at a later time.

Creating New Monitoring Policies

Prime Infrastructure monitoring policies monitor network device metrics and alert you of changing conditions before the issues impact their operation.

To create a new monitoring policy, follow these steps:

---

**Step 1** Choose Monitor > Monitoring Tools > Monitoring Policies > My Policies.

**Step 2** Click **Add**.

**Step 3** Select a monitoring policy from the Policy Types menu.

**Step 4** Enter a name for the new policy.

**Step 5** Under Parameters and Thresholds, specify the threshold values for which you want Prime Infrastructure to issue an alarm when they are reached.

**Step 6** Click:
- **Save and Activate** to save and activate the policy immediately on the selected devices.
- **Save and Close** to save the policy and activate it at a later time.
GETVPN Monitoring Policies

For the GETVPN policy type, Prime Infrastructure uses metrics described in Table 15-4.
<table>
<thead>
<tr>
<th>GETVPN Monitoring Parameters</th>
<th>MIB</th>
<th>MIB Objects Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>CISCO-GDOI-MIB</td>
<td>cgmgdoiGroupIdTable</td>
</tr>
<tr>
<td>Group ID</td>
<td></td>
<td>cgmgdoiGroupName, cgmgdoiGroupIdValue, cgmgdoiGroupIdType, cgmgdoiGroupIdLength</td>
</tr>
<tr>
<td>Group ID Type</td>
<td></td>
<td>cgmgdoiKeyServerTable</td>
</tr>
<tr>
<td>Group ID Length</td>
<td></td>
<td>cgmgdoiGroupIdValue, cgmgdoiGroupIdType, cgmgdoiKeyServerIdValue, cgmgdoiKeyServerIdType, cgmgdoiKeyServerIdLength, cgmgdoiKeyServerActiveKEK, cgmgdoiKeyServerRekeysPushed</td>
</tr>
<tr>
<td>Key Server ID</td>
<td></td>
<td>cgmgdoiKsKekTable</td>
</tr>
<tr>
<td>Group Member ID</td>
<td></td>
<td>cgmgdoiGroupIdValue, cgmgdoiGroupIdType, cgmgdoiKeyServerIdValue, cgmgdoiKeyServerIdType, cgmgdoiKsKekIndex, cgmgdoiKsKekSPI, cgmgdoiKsKekSrcIdValue, cgmgdoiKsKekSrcIdType, cgmgdoiKsKekSrcIdLength, cgmgdoiKsKekDstIdValue, cgmgdoiKsKekDstIdType, cgmgdoiKsKekDstIdLength, cgmgdoiKsKekOriginalLifetime, cgmgdoiKsKekRemainingLifetime</td>
</tr>
</tbody>
</table>
Table 15-4  Monitor > Monitoring Tools > Monitoring Policies > GETVPN Metrics (continued)

<table>
<thead>
<tr>
<th>GETVPN Monitoring Parameters</th>
<th>MIB</th>
<th>MIB Objects Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active KEK</td>
<td>CISCO-GDOI-MIB</td>
<td>cgmGdoiKsTekSelectorTable</td>
</tr>
<tr>
<td>Rekeys Count</td>
<td></td>
<td>cgmGdoiGroupIdValue, cgmGdoiGroupIdType,</td>
</tr>
<tr>
<td>KEK Index</td>
<td></td>
<td>cgmGdoiKeyIdServerIdValue, cgmGdoiKeyIdServerIdType,</td>
</tr>
<tr>
<td>KEK SPI</td>
<td></td>
<td>cgmGdoiKsTekSelectorIndex, cgmGdoiKsTekSrcIdValue,</td>
</tr>
<tr>
<td>KEK Source ID</td>
<td></td>
<td>cgmGdoiKsTekSrcIdType, cgmGdoiKsTekSrcIdLength,</td>
</tr>
<tr>
<td>KEK Source ID Type</td>
<td></td>
<td>cgmGdoiKsTekDstIdValue, cgmGdoiKsTekDstIdLength,</td>
</tr>
<tr>
<td>KEK Source ID Length</td>
<td></td>
<td>cgmGdoiKsTekOriginalLifetime, cgmGdoiKsTekRemainingLifetime,</td>
</tr>
<tr>
<td>KEK Destination ID</td>
<td></td>
<td>cgmGdoiGmTable</td>
</tr>
<tr>
<td>KEK Destination ID Type</td>
<td></td>
<td>cgmGdoiGroupIdValue, cgmGdoiGroupIdType,</td>
</tr>
<tr>
<td>KEK Destination ID Length</td>
<td></td>
<td>cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmIdLength,</td>
</tr>
<tr>
<td>KEK Original Lifetime</td>
<td></td>
<td>cgmGdoiGmRegKeyIdServerIdValue,</td>
</tr>
<tr>
<td>KEK Remaining Lifetime</td>
<td></td>
<td>cgmGdoiGmRegKeyIdServerIdType,</td>
</tr>
<tr>
<td>TEK Selector Index</td>
<td></td>
<td>cgmGdoiGmRegKeyIdServerIdLength, cgmGdoiGmActiveKEK,</td>
</tr>
<tr>
<td>TEK Source ID</td>
<td></td>
<td>cgmGdoiGmKekTable</td>
</tr>
<tr>
<td>TEK Source ID Type</td>
<td></td>
<td>cgmGdoiGroupIdValue, cgmGdoiGroupIdType,</td>
</tr>
<tr>
<td>TEK Destination ID</td>
<td></td>
<td>cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmKekIndex,</td>
</tr>
<tr>
<td>TEK Destination ID Type</td>
<td></td>
<td>cgmGdoiGmKekSPI, cgmGdoiGmKekSrcIdValue,</td>
</tr>
<tr>
<td>TEK Destination ID Length</td>
<td></td>
<td>cgmGdoiGmKekSrcIdType, cgmGdoiGmKekSrcIdLength,</td>
</tr>
<tr>
<td>TEK Policy Index</td>
<td></td>
<td>cgmGdoiGmKekDstIdValue, cgmGdoiGmKekDstIdType,</td>
</tr>
<tr>
<td>TEK SPI</td>
<td></td>
<td>cgmGdoiGmKekDstIdLength, cgmGdoiGmKekOriginalLifetime,</td>
</tr>
<tr>
<td>TEK Original Lifetime</td>
<td></td>
<td>cgmGdoiGmKekRemainingLifetime,</td>
</tr>
<tr>
<td>TEK Remaining Lifetime</td>
<td></td>
<td>cgmGdoiGmKekSelectorTable</td>
</tr>
<tr>
<td>TEK Window Size</td>
<td></td>
<td>cgmGdoiGroupIdValue, cgmGdoiGroupIdType,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekSelectorIndex, cgmGdoiGmKekSrcIdValue,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekSrcIdType, cgmGdoiGmKekSrcIdLength,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekDstIdValue, cgmGdoiGmKekDstIdType,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekDstIdLength,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekPolicyTable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGroupIdValue, cgmGdoiGroupIdType,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekPolicyIndex, cgmGdoiGmKekSPI,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekOriginalLifetime,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekRemainingLifetime,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cgmGdoiGmKekWindowSize</td>
</tr>
</tbody>
</table>

DMVPN Monitoring Policies

For the DMVPN policy type, Prime Infrastructure uses metrics described in Table 15-5.
# Table 15-5  Monitor > Monitoring Tools > Monitoring Policies > DMVPN Metrics

<table>
<thead>
<tr>
<th>DMVPN Monitoring Parameters</th>
<th>MIB</th>
<th>MIB Objects Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Peer Physical IP</td>
<td>CISCO-IPSEC-FLOW-MONITOR-MIB</td>
<td>cipSecTunnelTable, cipSecTunRemoteAddr, cipSecTunInOctets, cipSecTunOutOctets</td>
</tr>
<tr>
<td>Decrypted Byte Count</td>
<td>NHRP-MIB</td>
<td>nhrpCacheTable, nhrpCacheInternetworkAddr, nhrpCacheHoldingTime, nhrpCacheNbmaAddr, nhrpCacheType</td>
</tr>
<tr>
<td>Encrypted Byte Count</td>
<td>IP-FORWARD-MIB</td>
<td>ipCidrRouteTable, ipCidrRouteNextHop, ipCidrRouteDest, ipCidrRouteMask</td>
</tr>
<tr>
<td>Remote Tunnel IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NHRP Expiration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Subnet IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Subnet Mask</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Nexus Virtual Port Channel (VPC) Health Monitoring Policy

The Nexus VPC health monitoring policy periodically fetches the configuration parameters from the primary VPC configured Nexus Switch and looks for any discrepancies in the configuration that can lead to inconsistencies, by correlating with the secondary VPC configured Nexus Switch. If inconsistencies are detected the monitoring policy generates an alarm and captures the details of the inconsistency at global level and VPC level. Table 15-6 shows the various Nexus VPC monitoring parameters.

Table 15-6  Monitor > Monitoring Tools > Monitoring Policies > Nexus VPC Health

<table>
<thead>
<tr>
<th>Category</th>
<th>Nexus VPC Monitoring Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Fault</td>
<td>stpModerstp&lt;br&gt;Disabled&lt;br&gt;stpMstRegionName&lt;br&gt;stpMstRegionRevision&lt;br&gt;stpMstRegionVlanMap&lt;br&gt;stpLoopguard&lt;br&gt;stpBridgeAssurance&lt;br&gt;stpEdgePortType&lt;br&gt;bpdudFilterGuard&lt;br&gt;stpMstSimulatePvst&lt;br&gt;passVlans</td>
</tr>
<tr>
<td>VPC Fault</td>
<td>VpcCardType&lt;br&gt;OperationalPortMode&lt;br&gt;Mode&lt;br&gt;LacpMode&lt;br&gt;InterfaceType&lt;br&gt;AdminPortMode&lt;br&gt;Speed&lt;br&gt;Duplex&lt;br&gt;Mtu&lt;br&gt;NativeVlan&lt;br&gt;StpPortType&lt;br&gt;StpPortGuard&lt;br&gt;StpMstSimulatePvst</td>
</tr>
</tbody>
</table>

LISP Monitoring Policy

For the LISP monitoring policy type, Prime Infrastructure uses the metrics shown in Table 15-7.

Table 15-7  Monitor > Monitoring Tools > Monitoring Policies > LISP Monitoring

<table>
<thead>
<tr>
<th>LISP Monitoring Parameters</th>
<th>MIB</th>
<th>MIB Objects Included</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISP Map Cache Size</td>
<td>LISP-MIB</td>
<td>lispFeaturesMapCacheSize</td>
</tr>
<tr>
<td>LISP Map Cache Limit</td>
<td>LISP-MIB</td>
<td>lispFeaturesMapCacheLimit</td>
</tr>
</tbody>
</table>

You can view the polled data in the Device Lisp Map Cache Entries dashlet under Device dashboard and in the Top N Lisp Map Cache Entries dashlet under the Network Devices dashboard.
Monitoring Third-Party Devices By Polling MIBs

You can design custom MIB polling policies to monitor third-party or Cisco devices and device groups. You can also create custom MIB policies to monitor device features for which Prime Infrastructure doesn’t provide default policies. Using this feature, you can:

- Upload the SNMP MIB for the device type, then choose devices and attributes to poll and the polling frequency.
- Upload a single MIB definition file or a group of MIBs with their dependencies as a ZIP file.

**Note** Ensure that you upload all the dependencies of the MIB, before uploading the MIB. You can also upload the MIB along with its dependencies in a ZIP file.

- Display the results as a line chart or a table.

This feature allows you to easily repeat polling for the same devices and attributes and customize the way Cisco devices are polled using SNMP.

You can create a maximum of 25 custom MIB polling policies. There is no limitation in the number of MIB files uploaded.

To create custom MIB polling policies, follow these steps:

---

**Step 1** Choose **Monitor > Monitoring Tools > Monitoring Policies > My Policies**, then click **Add**.

**Step 2** From the Policy Types menu, select **Custom MIB Polling**.

**Step 3** Enter a name for the policy.

**Step 4** Under the MIB Selection tab, specify the polling frequency and enter the MIB information.

- If Prime Infrastructure doesn’t have the specific MIB you want to monitor, download the MIBs you want to monitor from the following URL:
- To upload a MIB, specify a filename extension only if you are uploading a ZIP file.
  Regardless of the device, the extensions .ZIP, .MIB and .MY are allowed.
- If you are uploading a ZIP file, ensure that all dependent MIB files are either included in the ZIP or already present in the system.
- Ensure your upload file and the MIB definition have the same name (for example: Do not rename the ARUBA-MGMT-MIB definition file to ARUBA_MGMT). If you are uploading a ZIP file, you may name it as you please, but the MIB files packaged inside it must also follow this convention (for example: MyMibs.zip is acceptable, as long as all MIB files in the ZIP match their MIB names).

**Step 5** To test the policy you created on a device before activating it, click the **Test** tab and select a device on which to test the new policy.

**Step 6** Click **Save and Activate** to immediately activate the policy on the devices specified.

**Step 7** To view the MIB polling data, create a generic dashlet (see **Creating Generic Dashlets**) using the name of the policy that you created.

To view the SNMP polling data for ASR devices, you should use the `show platform hardware qfp active datapath utilization | inc Processing` command for CPU utilization and `show platform hardware qfp active infrastructure exmem statistics | sec DRAM` command for memory utilization.
Example: Monitoring IP SLA

You can create a monitoring policy to view IP service levels for network-based applications and services. There are approximately seven IP SLA-related MIBs. In this example, the video MIB only is monitored.

---

**Step 1**  Download the IP SLA video MIB from the following URL:

**Step 2**  Choose **Monitor > Monitoring Policies > My Policies**, then click **Add**.

**Step 3**  Click **Custom MIB Polling**.

**Step 4**  Enter a name for the policy.

**Step 5**  Under the MIB Selection tab, click **Upload MIB** and navigate to the MIB that you uploaded in Step 1.

**Step 6**  From the Tables pulldown menu, select a table, then select the specific metrics to monitor.

**Step 7**  To test the policy you created on a device before activating it, click the **Test** tab and select a device on which to test the new policy.

**Step 8**  Select the devices for which you want to monitor IP SLA metrics.

**Step 9**  Click **Save and Activate** to immediately activate the policy on the devices specified.

**Step 10**  To monitor this information from a dashboard, you need to create a generic dashlet. See **Creating Generic Dashlets** for more information.

---

Polled Data in Dashlets and Reports

When viewing polled data from devices, consider the following scenario:

- Device 1 data is polled from the last 6 hours.
- Device 2 data is polled from the last 2 days.

When you filter dashlets or reports to show data from the past 2 days, only the data from Device 2 is displayed.

If you filter dashlets and reports by devices and time frame, then data for both devices is displayed.
Monitoring Alarms

An alarm is a Cisco Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the condition no longer occurs.

- What Is an Event?
- What Is an Alarm?
- Defining Alarm Thresholds
- Where to Find Alarms
- Display Options
- Changing Alarm Status
- Changing Alarm and Event Options
- Configuring Alarm Severity Levels
- Customizing Alarms and Events For Traps
- What is an Alarm Policy?
- Getting Help for Alarms
- Viewing Syslogs

What Is an Event?

An event is an occurrence or detection of some condition in or around the network. An event is a distinct incident that occurs at a specific point in time. Examples of events include:

- Port status change
- Device reset
- Device becomes unreachable by the management station

An event can also result from:

- A fault that is an error, failure, or exceptional condition in the network. For example, when a device becomes unreachable, an unreachable event is triggered.
- A fault clearing. For example, when a device state changes from unreachable to reachable, a reachable event is triggered.

One or more events may generate an abnormal state or alarm. The alarm can be cleared, but the event remains. You can view the list of events using the Event Browser.
What Is an Alarm?

Choose **Monitor > Monitoring Tools > Alarms & Events**, then click **Events** to access the Events Browser page.

**Event Creation**

Prime Infrastructure maintains an event catalog and decides how and when an event is created and whether to associate an alarm with the event. Multiple events can be associated with the same alarm.

Prime Infrastructure discovers events in the following ways:

- By receiving notification events and analyzing them; for example, syslog and traps.
- By automatically polling devices and discovering changes; for example, device unreachable.
- By receiving events when a significant change occurs on the Prime Infrastructure server; for example, rebooting the server.

Incoming event notifications (traps and sylogs) are identified by matching the event data to predefined patterns. A trap or syslog is considered supported by Prime Infrastructure if it has matching patterns and can be properly identified. If the event data does not match predefined patterns, the event is considered unsupported, and it is dropped.

Faults are discovered by Prime Infrastructure through polling, traps, or syslog messages. Prime Infrastructure maintains the context of all faults and ensures that duplicate events or alarms are not maintained in the Prime Infrastructure database.

The following table provides examples of when Prime Infrastructure creates an event.

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Prime Infrastructure Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00AM PDT Dec 1, 2014</td>
<td>Device A becomes unreachable.</td>
<td>Creates a new unreachable event on device A.</td>
</tr>
<tr>
<td>10:30AM PDT Dec 1, 2014</td>
<td>Device A continues to be unreachable.</td>
<td>No change in the event status.</td>
</tr>
<tr>
<td>10:45AM PDT Dec 1, 2014</td>
<td>Device A becomes reachable.</td>
<td>Creates a new reachable event on device A.</td>
</tr>
<tr>
<td>11:00AM PDT Dec 1, 2014</td>
<td>Device A stays reachable.</td>
<td>No change in the event status.</td>
</tr>
<tr>
<td>12:00AM PDT Dec 1, 2014</td>
<td>Device A becomes unreachable.</td>
<td>Creates a new unreachable event on device A.</td>
</tr>
</tbody>
</table>

**Recurring Alarms and Events**

To reduce the amount of unnecessary alarms and events, Prime Infrastructure detects the underlying causes of an event, and then modifies when it issues alarms and events if the devices have any of the problems. For example, for module or link faults, if a module is down, Prime Infrastructure creates one Module Down alarm only, and associates all of the interfaces’ link down events to the Module Down alarm. When the module state is restored, Prime Infrastructure clears the module alarm and all interface messages are associated to the cleared alarm.

When several link-up and link-down traps are received for the same interface, within a short time period, then Prime Infrastructure detects those traps and creates a Flapping event.

**What Is an Alarm?**

An alarm is a Prime Infrastructure response to one or more related events. If an event is considered of high enough severity (critical, major, minor, or warning), Prime Infrastructure raises an alarm until the resulting condition no longer occurs.
One or more events can result in a single alarm being raised. An alarm is created in the following sequence:

1. A notification is triggered when a fault occurs in the network.
2. An event is created, based on the notification.
3. An alarm is created after verifying that there is no active alarm corresponding to this event.

**Event and Alarm Association**

Prime Infrastructure maintains a catalog of events and alarms. This catalog contains a list of events and alarms managed by Prime Infrastructure, and the relationship among the events and alarms. Events of different types can be attached to the same alarm type.

When a notification is received:

1. Prime Infrastructure compares an incoming notification against the event and alarm catalog.
2. Prime Infrastructure decides whether to raise an event.
3. If an event is raised, Prime Infrastructure decides if the event triggers a new alarm or if it is associated with an existing alarm.

A new event is associated with an existing alarm if the new event is of the same type and occurs on the same source.

**Alarm Status**

Table 16-1 provides alarm status descriptions.

<table>
<thead>
<tr>
<th>Alarm Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not acknowledged</td>
<td>When an event triggers a new alarm or a new event is associated with an existing alarm.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>When you acknowledge an alarm, the status changes from Not acknowledged to Acknowledged.</td>
</tr>
<tr>
<td>Cleared</td>
<td>A cleared alarm can involve any of the following:</td>
</tr>
<tr>
<td></td>
<td>- Auto-clear from the device—The fault is resolved on the device and an event is triggered for the device. For example, a device-reachable event clears a device-unreachable event. This, in turn, clears the device-unreachable alarm.</td>
</tr>
<tr>
<td></td>
<td>- Manual-clear from Prime Infrastructure users—You can manually clear an active alarm without resolving the fault in the network. A clearing event is triggered and the alarm is cleared.</td>
</tr>
<tr>
<td></td>
<td>- If a fault continues to exist in the network, a new event and alarm are created subsequently, based on event notification (traps/syslogs).</td>
</tr>
</tbody>
</table>

**Event and Alarm Severity**

Each event has an assigned severity. Events fall broadly into the following severity categories, each with an associated color in Prime Infrastructure:

- Flagging (indicates a fault)—Critical (red), Major (orange), Minor (yellow), or Warning (sky blue).
- Informational—Info (blue). Some informational events clear flagging events.

For example, a Link Down event might be assigned Critical severity, while its corresponding Link Up event will be Cleared severity.

In a sequence of events, the event with the highest severity determines the severity of the alarm.
Defining Alarm Thresholds

Use monitoring templates to define thresholds. When the thresholds that you specify are reached, Prime Infrastructure issues an alarm. See Creating Monitoring Policies and Thresholds for information about defining thresholds.

Where to Find Alarms

Table 16-2 lists where you can find alarms.

<table>
<thead>
<tr>
<th>Location in GUI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor &gt; Monitoring Tools &gt; Alarms &amp; Events</td>
<td>Displays a new page listing all alarms with details such as severity, status, failure source, timestamp, Device Timestamp, owner, category, and condition. You can change the status of alarms and assign, annotate, delete, specify email notifications from this page and use the troubleshoot functionality to devices from Prime Infrastructure. If you enable Alarm Badging, Prime Infrastructure displays severity icons next to the device groups. See Displaying Alarm Icons.</td>
</tr>
<tr>
<td>Toolbar on top right of the Prime Infrastructure window</td>
<td>The red box on the top right of the Prime Infrastructure window displays the total number of critical alarms currently detected by Prime Infrastructure. You can click on the box to open the Alarm Summary. See Customizing the Alarm Summary.</td>
</tr>
<tr>
<td>From device 360° view</td>
<td>On the Alarms tab, when you hover the mouse over the Failure Source field, the crosshair icon appears. Click the icon to see the 360° view of the device. Or, on the Alarm browser, when you hover the mouse over the Failure Source field, the crosshair icon appears. Click the icon to see the 360° view of the device.</td>
</tr>
<tr>
<td>Dashboard &gt; Overview &gt; Incidents</td>
<td>Displays dashlets that contain alarm summary information, top n sites with the most alarms, top n alarm types, device reachability status, syslog watch, and syslog summary.</td>
</tr>
<tr>
<td>Dashboard &gt; Network Summary &gt; Incidents</td>
<td>Displays dashlets that contain Alarms, Top N Alarm Types, Syslog Summary and Top N Event Types.</td>
</tr>
<tr>
<td>Dashboard &gt; Data Center &gt; Compute</td>
<td>Displays Compute Resources Summary dashlet which shows alarms associated with each Compute Resource.</td>
</tr>
<tr>
<td>Inventory &gt; Device Management &gt; Compute Devices &gt; Compute Resources &gt; Clusters &gt; Cluster Detail Page</td>
<td>Displays Severity, Status, Timestamp and Description of the Alarms in the Alarms area.</td>
</tr>
</tbody>
</table>
Display Options

The following sections explain the various ways you can modify how alarms, events, and syslogs are displayed:

- Viewing Options for Alarms, Events, and Syslogs
- Displaying Alarm Icons
- Changing Alarm Display Behavior
- Modifying Alarm Failure Source Pattern

Viewing Options for Alarms, Events, and Syslogs

When you choose Monitor > Monitoring Tools > Alarms & Events, then click any of the tabs at the top of the page (Alarms, Events, or Syslogs), you can click on either of the following viewing modes:

- **Show Latest 4000 Alarms**—Prime Infrastructure displays the most recent alarms, events, or syslogs (depending on which tab you clicked), based on the timestamp when it was last modified. The Most Recent cache supports till 4000 alarms that can be displayed in the Show Latest 4000 Alarms. If a newer alarm, event, or syslog occurs, Prime Infrastructure removes an older item from the list and adds the most recent one.

- **Show All**—Prime Infrastructure retrieves all alarms, events, or syslogs from the database and displays them.

You can use filters on either view.

If there are more than 200,000 rows of data on the Alarms, Events, or Syslog page, the global toolbar displays \(200000 \text{ of } N\) where \(N\) is the total number of rows in the table. If you hover your cursor over \(200000 \text{ of } N\), a message appears saying that “Only the first 200,000 rows are displayed. Use the table filter controls to display a smaller result set.”
Displaying Alarm Icons

To have Prime Infrastructure display alarm severity icons next to the device groups on the Monitor > Monitoring Tools > Alarms & Events page, you need to enable Alarm Badging. This feature is disabled by default because it could impact performance if Prime Infrastructure is monitoring more than 2,000 devices with more than 10,000 active alarms. If you notice performance degradation issues, we suggest you disable this feature.

**Step 1** Click your login name at the top-right of the screen and choose My Preferences.

**Step 2** Click the checkbox next to Enable Alarm Badging on Alarms & Events page.

**Step 3** Click Save.

Changing Alarm Display Behavior

Prime Infrastructure provides user preference settings that let you control whether:

- Automatically refreshes the Alarms and Events page.
- Prime Infrastructure displays prompts and warning messages when you acknowledge an alarm or clear all alarms of a condition.
- Cleared alarm conditions are always set to the “Information” severity level.

**Step 1** Click the Settings icon and choose My Preferences.

**Step 2** Click Alarms & Events tab.

**Step 3** If you want Alarms/Events/Syslog page to automatically refresh at a periodic interval, select the Automatically refresh Alarms & Events page.

**Step 4** If you do not want the warning message to appear whenever you acknowledge an alarm, select the Disable Alarm Acknowledge Warning Message check box. Note that the warning message displays as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled.

**Step 5** If you do not want to be prompted to confirm each time you clear an alarm condition, select the Disable confirmation prompt for “Clear all of this condition” check box. Note that the warning displays as a reminder that you are clearing all occurrences of the specified condition.

**Step 6** If you do not want to be prompted to confirm the severity change each time you clear an alarm condition, select the Disable “Set severity to Information?” prompt for “Clear all of this condition” check box.

**Step 7** Click Save.

Related Topics

- Customizing the Alarm Summary
- Customizing Alarms and Events For Traps
Modifying Alarm Failure Source Pattern

- Select the category you need to customize and click **Edit**.
- Select the failure source pattern from the options available and click **OK**.
- Select the category for which you want to customize the separator and click **Edit Separator**. Select one of the options available, then click **OK**.

The alarms generated for the selected category will have the customized pattern that you set. For example, if you select the Clients category, and then edit the separator to be #, when any supported client alarm is generated, when you select **Monitor > Monitoring Tools > Alarms and Events**, the Failure Source column for that alarm will be **MACaddress#Name**.

**Note**

- Failure Source is not supported for Custom traps and Custom syslog translation.
- Failure Source is not supported for Syslog generated events.

Customizing the Alarm Summary

Prime Infrastructure provides user settings that control the information shown in the Alarm Summary box (shown in the top right of the Toolbar at the top on the Prime Infrastructure window) and in the Alarm Summary pop-up page displayed when you click on the Alarm Summary box. These include:

- How often the alarm count is refreshed in the Alarm Summary box and page.
- Which category of alarm to track as the default alarm category shown in the Alarm Summary box.
- Which categories of alarms to include in the Alarm Summary page, and in the total displayed in the Alarm Summary box.

**Step 1**

Click the **Settings** icon and choose **My Preferences**.
You can also access the User Preferences page by clicking the arrow next to your login name in the Global Toolbar at the top right.

**Step 2**

To change the Alarm Summary refresh frequency: In the **Refresh Alarm count in the Alarm Summary** drop down list, choose a refresh frequency (every 5 seconds, 15 seconds, 30 seconds, 1 minute, 2 minutes, or 5 minutes).

**Step 3**

To select the alarm categories to display in the Alarm Summary box and pop-up page:

a. Click **Edit Alarm Categories**. The Select Alarm Categories pop-up displays.

b. In the **Default Category to display** drop-down, choose the default category whose total alarm count you want to display in the Alarm Summary box. For example: Choose “AP Rogue” to have the Alarm Summary box display the count for AP Rogue alarms only. Choose “Alarm Summary” to have the box display a count of all alarms in all selected categories and subcategories.

c. In the pick list under the **Show** drop-down, choose the checkbox next to each category or sub-category of alarm that you want to include in the Alarm Summary popup page.

If **Default Category to display** is set to “Alarm Summary”, the alarm totals shown will be the total of all critical alarms for all the categories and sub-categories you select in the pick list. If any other category or sub-category is selected as the Default Category, the box displays totals only for that category.
Changing Alarm Status

You can remove an alarm from the list of alarms by changing its status to Acknowledged or Cleared. No e-mails will be generated for these alarms.

**Step 1** Choose **Monitor > Monitoring Tools > Alarms & Events**. By default, the Alarms tab is selected.

**Step 2** Select an alarm, then choose one of the following options under **Change Status**:

- **Acknowledge**—Removes the alarm from the Alarms list and prevents the alarm from being counted as an active alarm on the Alarm Summary page or any alarms list.

- **Unacknowledge**—Returns the alarm to its active alarm state on the Alarm Summary page and all alarms lists.

- **Clear**—Sets the alarm state to Cleared. Cleared alarms remain in the Prime Infrastructure database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

- **Clear all of this Condition**—Sets the alarm state to Cleared for all alarms with the same Condition as the alarm you selected.

  After you click **Yes** to confirm that you want to clear all alarms of the specified condition, a dialog appears asking if you want to change the severity for the selected alarm condition to Informational. This prevents Prime Infrastructure from issuing alarms for the specified condition. To later reset the condition’s severity, choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear > Severity Configuration** and modify the severity.

**Related Topics**
- Configuring Alarm Severity Levels
- When to Acknowledge Alarms
- Including Acknowledged and Cleared Alarms in Searches

When to Acknowledge Alarms

You may want certain alarms to be removed from the Alarms list. For example, if you are continuously receiving an interference alarm from a certain device, you may want to stop that alarm from being counted as an active alarm on the Alarm Summary page or any alarms list. In this scenario, you can find the alarm for the device in the Alarms list, select an alarm and choose **Change Status > Acknowledge**.
If the device generates a new violation on the same interface, Prime Infrastructure does not create a new alarm, and the Alarm Summary page shows no new alarms. However, if the interference violation is created on another interface, a new alarm is created.

By default, acknowledged alarms are not displayed on either the Alarm Summary page or in any alarm list. Also, no emails are generated for acknowledged alarms. By default, acknowledged alarms are not included for any search criteria. To change this default, go to the Administration > Settings > System Settings > Alarms and Events page and disable the Hide Acknowledged Alarms preference.

When you acknowledge an alarm, a warning message appears as a reminder that a recurrence of the problem does not generate another alarm unless this functionality is disabled. Click the Settings icon and choose My Preferences page to disable this warning message.

You can also search for all previously acknowledged alarms to reveal the alarms that were acknowledged during the last seven days. Prime Infrastructure automatically deletes cleared alerts that are more than seven days old, so your results can show activity for only the last seven days. Until an existing alarm is deleted, a new alarm cannot be generated for any managed entity for which Prime Infrastructure has already generated an alarm.

**Including Acknowledged and Cleared Alarms in Searches**

By default, acknowledged and cleared alarms are not included for any search criteria. To change this default, choose Administration > Settings > System Settings > Alarms and Events and disable the Hide Acknowledged Alarms or Hide Cleared Alarms preference.

Cleared alarms remain in the Prime Infrastructure database, but in the Clear state. You clear an alarm when the condition that caused it no longer exists.

**Changing Alarm and Event Options**

You might want to change the schedule for deleting alarms, the alarm severities that are displayed, or alarm email options.

To change alarm and event options, follow these steps:

1. **Step 1** Choose Administration > Settings > System Settings.
2. **Step 2** From the left sidebar menu, choose Alarms and Events.
3. **Step 3** Change the alarm or event settings, then click Save.

**Configuring Alarm Severity Levels**

A newly generated alarm has a default severity level that you might want to change.

To configure an alarm’s severity level, follow these steps:

1. **Step 1** Choose Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear.
2. **Step 2** Choose Severity Configuration.
Customizing Alarms and Events For Traps

You can enable Prime Infrastructure to recognize additional traps and to customize how Prime Infrastructure creates events and alarms for these traps. You can specify a trap notification name or syslog message identifier, and specify the event severity, category, and message to use when the specified trap is received. Prime Infrastructure creates an event with the settings you specify.

**Step 1** Choose Monitor > Monitoring Tools > Alarms & Events.

**Step 2** Click the Events tab.

**Step 3** Click Custom Trap Event. The Custom Trap Events window opens displaying any previously created custom trap events.

**Step 4** Click Add.

**Step 5** Select a MIB from the menu, which includes all MIBs that are not fully supported, or click Upload New MIB to upload a MIB file.

If you upload a new MIB file, wait approximately 15 seconds, then click Refresh MIBs to have the newly added MIB added to the MIB drop-down list.

**Step 6** Select a Notification Name from the list of unsupported notification names included in the selected MIB.

**Step 7** In the Event Description field, enter the text you want displayed in the Description column for the events that are generated from traps with the selected notification name.

**Step 8** Select a Default Severity level, then click OK.

Prime Infrastructure creates a new event type and alarm condition for the specified trap.

**Related Topic**
- Modifying a Customized Trap Event

**Modifying a Customized Trap Event**

You can modify a previously created customized trap event.

**Step 1** Choose Monitor > Monitoring Tools > Alarms & Events.

**Step 2** Click the Events tab.

**Step 3** Click Custom Trap Event. The Custom Trap Events window opens displaying any previously created custom trap events.

**Step 4** Select the custom trap event you want to modify, then click Edit.
What is an Alarm Policy?

An Alarm Policy is a filtering method that allows you to control the alarms on network conditions, thereby reducing noise in the system.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as active.

Prime Infrastructure supports the following Alarm Policies:

- **Interface Alarm Policy**—Allows you to activate or suppress the interface alarms on interface-related events, device groups, and port groups.
- **Controller Alarm Policy**—Allows you to activate or suppress the alarms on controller-related events for the selected device groups.
- **Access Points Alarm Policy**—Allows you to activate or suppress the AP alarms on AP-related events, device groups, and alarm thresholds.
- **Layer2 Switch**—Allows you to activate and suppress alarms on Layer 2 switch-related events for the selected device groups.
- **Wired Infrastructure**—Allows you to activate and suppress alarms on Wired Infrastructure-related events for the selected device groups.

The new alarm policies will not be applicable for the alarms already generated by Prime Infrastructure. You must delete or clear the existing alarms for the alarm policy to be effective in Prime Infrastructure.

**Customizing Interface Alarm Policy**

You can activate or suppress the types of events, device groups and port groups on which you want the alarms to be generated or ignored.

To edit the Interface Alarm Policy, follow these steps:
What is an Alarm Policy?

Step 1  Choose Monitor > Monitoring Tools > Alarm Policies.

Step 2  Check the Interface check box and then click Edit.

The Edit Interface Alarm Policy page displays the default list of events that you want to modify.

Step 3  Click the Activated or Suppressed toggle button to activate or suppress the alarm for the required event.

To perform a bulk edit, select the required Events check boxes and select Activate or Suppress from the Activate drop-down list.

Step 4  Set the required severity for an alarm from the Severity drop-down list.

To perform a bulk edit, select the required Events check boxes and select a severity from the Change Severity drop-down list.

Step 5  In the Auto Clear Duration field, enter the value in hours for the alarm to clear automatically for an event.

To perform a bulk edit, select the required Events check boxes and edit the Alarm Auto Clear field.

Alternatively, you can choose Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear to set the severity and auto clear duration for an alarm.

Step 6  Click Save and Activate, or click Next to continue with the Device Groups page.

Step 7  Click the All devices are selected or No devices are selected toggle button to activate or suppress the events selected in Step 3 for the particular device groups. Some devices are selected is displayed only when a few devices in a device group are selected.

To perform a bulk edit, select the required device group check boxes and select Activate or Suppress from the Activate drop-down list.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as active.

Step 8  Click Save and Activate, or click Next to continue with the Ports Group page.

Step 9  Click the All port types are selected or No port types are selected toggle button to activate or suppress the selected events. Network events on the ports belonging to the unselected groups will be suppressed. Some port types are selected is displayed only when a few ports in a port group are selected.

To perform a bulk edit, select the required port group check boxes and select Activate or Suppress from the Activate drop-down list.

Step 10  Click Save and Activate.

Related Topics

- What is an Alarm Policy?
- Customizing Controller Alarm Policy
- Customizing Access Point Alarm Policy
- Customizing Layer2 Switch Alarm Policy
- Customizing Wired Infrastructure Alarm Policy
- Viewing the Alarm Policy Summary
- Restoring Default Settings
Customizing Controller Alarm Policy

You can activate or suppress the types of events and device groups for which you want the alarms to be generated or ignored. If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as active.

To edit the Controller Alarm Policy, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Alarm Policies**.

**Step 2** Check the **Controller** check box and then click **Edit**.

The **Edit Controller Alarm Policy** page displays the default list of events that you want to modify.

**Step 3** Click the **Activated** or **Suppressed** toggle button to activate or suppress the alarm for the required event.

To perform a bulk edit, select the required **Events** check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

**Step 4** Set the required severity for an alarm from the **Severity** drop-down list.

To perform a bulk edit, select the required **Events** check boxes and select a severity from the **Change Severity** drop-down list.

**Step 5** In the **Auto Clear Duration** field, enter the value in hours for the alarm to clear automatically for an event.

To perform a bulk edit, select the required **Events** check boxes and edit the **Alarm Auto Clear** field.

Alternatively, you can choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear** to set the severity and auto clear duration for an alarm.

**Step 6** Click **Save and Activate**, or click **Next** to continue with the **Device Groups** page.

**Step 7** Click the **All devices are selected** or **No devices are selected** toggle button to activate or suppress the events selected in **Step 3** for the particular device groups. **Some devices are selected** is displayed only when a few devices in a device group are selected.

To perform a bulk edit, select the required device group check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as active.

**Step 8** Click **Save and Activate**.

**Related Topics**

- What is an Alarm Policy?
- Customizing Interface Alarm Policy
- Customizing Access Point Alarm Policy
- Customizing Layer2 Switch Alarm Policy
- Customizing Wired Infrastructure Alarm Policy
- Viewing the Alarm Policy Summary
- Restoring Default Settings
Customizing Access Point Alarm Policy

You can activate or suppress the types of events and device groups for which you want the alarms to be generated or ignored. Also, you can set the threshold value to control the alarms.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as active.

To edit the Access Point Alarm Policy, follow these steps:

---

**Step 1** Choose Monitor > Monitoring Tools > Alarm Policies.
**Step 2** Check the Access Point policy name, then click the Edit Policy link.

The Edit Access Point Alarm Policy page displays the default list of events that you want to modify.

**Step 3** Click the Activated or Suppressed toggle button to activate or suppress the alarm for the required event.
To perform a bulk edit, select the required Events check boxes and select Activate or Suppress from the Activate drop-down list.

**Step 4** Set the required severity for an alarm from the Severity drop-down list.
To perform a bulk edit, select the required Events check boxes and select a severity from the Change Severity drop-down list.

**Step 5** In the Auto Clear Duration field, enter the value in hours for the alarm to clear automatically for an event.
To perform a bulk edit, select the required Events check boxes and edit the Alarm Auto Clear field.
Alternatively, you can choose Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear to set the severity and auto clear duration for an alarm.

**Step 6** Click Save and Activate, or click Next to continue with the Device Groups page.

**Step 7** Click the All devices are selected or No devices are selected toggle button to activate or suppress the events selected in Step 3 for the particular device groups. Some devices are selected is displayed only when a few devices in a device group are selected.
To perform a bulk edit, select the required device group check boxes and select Activate or Suppress from the Activate drop-down list.

**Step 8** Click Save and Activate, or click Next to continue with the Alarm Threshold page.

**Step 9** Enter the threshold value in percentage in the AP Down Group Impact % field of the required device group to set the threshold so that alarm will be generated only when the specified percentage of APs are dissociated in the selected groups.

**Step 10** Enter the time in minutes in the AP Down Sustain Time (Minutes) field of the required device group to set the maximum duration after which the alarm can be generated for an AP that goes down or not reachable.

---

**Note** If you specify both AP Down Group Impact % and AP Down Sustain Time (Minutes) for a device group, then an alarm will be generated only when the specified percentage of APs dissociated from the controller are down for the specified duration. See Understanding Access Point Alarm Policy Thresholds.
Step 11  Click **Save and Activate**.

**Related Topics**
- Understanding Access Point Alarm Policy Thresholds
- What is an Alarm Policy?
- Customizing Interface Alarm Policy
- Customizing Controller Alarm Policy
- Customizing Layer2 Switch Alarm Policy
- Customizing Wired Infrastructure Alarm Policy
- Viewing the Alarm Policy Summary
- Restoring Default Settings

**Understanding Access Point Alarm Policy Thresholds**

Specifying an AP Down Group Impact percentage and/or an AP Down Sustain Time duration for a device group modifies when alarms are created as described below:

- If you select an AP Down Group Impact percentage for a device group, any AP dissociated alarms for APs in the group are suppressed.
  
  When the percentage of down APs in the group exceeds the threshold percentage, Prime Infrastructure generates an ImpactedGroup alarm. When the percentage of down APs falls below the threshold, the ImpactedGroup alarm is cleared.

- If you specify an AP Down Sustain Time duration only for a device group, when an AP dissociated alarm event occurs for an AP within the group, Prime Infrastructure creates an alarm only if the AP dissociated alarm does not clear before the sustain time has elapsed.

- If you specify both an AP Down Group Impact percentage and an AP Down Sustain Time duration:
  - If an AP dissociated alarm event occurs for an AP within the group, Prime Infrastructure does not generate an alarm.
  - If the AP dissociated alarm event does not clear before the specified time has elapsed, the group is considered as a down AP.
  - If the percentage of APs in the group that have AP dissociated alarms that have not cleared before the configured time exceeds the threshold percentage, Prime Infrastructure generates an ImpactedGroup alarm.
  - If a clearing event for one of the AP dissociated alarms occurs for one of the APs that are considered down by the Group, the ImpactedGroup alarm is cleared.

The following example explains the policy behavior when you specify an AP Down Group Impact percentage and an AP Down Sustain Time duration for a device group.

Floor 1 has 3 APs—AP A, AP B, and AP C and the Alarm Thresholds have the following values:
- AP Down Group Impact %: 50%
- AP Down Sustain Time (Minutes): 5 minutes

1. AP A sends AP_DISASSOCIATED.
2. After 3 minutes, AP B sends AP_DISASSOCIATED.
3. After 5 minutes, ‘AP A’ AP_DISASSOCIATED expires.
4. After 8 minutes, ‘AP B’ AP_DISASSOCIATED expires.

Prime Infrastructure generates an Impacted Group alarm because the 50% AP Down Group Impact threshold has been crossed.

**Customizing Layer2 Switch Alarm Policy**

You can activate or suppress the types of events and device groups on which you want the alarms to be generated or ignored.

To edit the Layer2 Switch Alarm Policy, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Alarm Policies**.

**Step 2** Check the **Layer2 Switch** check box and then click **Edit**. The **Edit Layer2 Switch Alarm Policy** page displays the default list of events that you want to modify.

**Step 3** Click the **Activated** or **Suppressed** toggle button to activate or suppress the alarm for the required event. To perform a bulk edit, select the required **Events** check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

**Step 4** Set the required severity for an alarm from the **Severity** drop-down list. To perform a bulk edit, select the required **Events** check boxes and select a severity from the **Change Severity** drop-down list.

**Step 5** In the **Auto Clear Duration** field, enter the value in hours for the alarm to clear automatically for an event. To perform a bulk edit, select the required **Events** check boxes and edit the **Alarm Auto Clear** field. Alternatively, you can choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear** to set the severity and auto clear duration for an alarm.

**Step 6** Click **Save and Activate**, or click **Next** to continue with the **Device Groups** page.

**Step 7** Click the **All devices are selected** or **No devices are selected** toggle button to activate or suppress the events selected in **Step 3** for the particular device groups. **Some devices are selected** is displayed only when a few devices in a device group are selected.

To perform a bulk edit, select the required device group check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as **active**.

**Step 8** Click **Save and Activate**.

**Related Topics**
- What is an Alarm Policy?
- Customizing Interface Alarm Policy
- Customizing Controller Alarm Policy
- Customizing Access Point Alarm Policy
Customizing Wired Infrastructure Alarm Policy

You can activate or suppress the types of events and device groups on which you want the alarms to be generated or ignored.

To edit the Wired Infrastructure Alarm Policy, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Alarm Policies**.

**Step 2** Check the **Wired Infrastructure** check box and then click **Edit**.

The **Edit Wired Infrastructure Alarm Policy** page displays the default list of events that you want to modify.

**Step 3** Click the **Activated** or **Suppressed** toggle button to activate or suppress the alarm for the required event.

To perform a bulk edit, select the required **Events** check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

**Step 4** Set the required severity for an alarm from the **Severity** drop-down list.

To perform a bulk edit, select the required **Events** check boxes and select a severity from the **Change Severity** drop-down list.

**Step 5** In the **Auto Clear Duration** field, enter the value in hours for the alarm to clear automatically for an event.

To perform a bulk edit, select the required **Events** check boxes and edit the **Alarm Auto Clear** field.

Alternatively, you can choose **Administration > Settings > System Settings > Alarms and Events > Alarm Severity and Auto Clear** to set the severity and auto clear duration for an alarm.

**Step 6** Click **Save and Activate**, or click **Next** to continue with the **Device Groups** page.

**Step 7** Click the **All devices are selected** or **No devices are selected** toggle button to activate or suppress the events selected in **Step 3** for the particular device groups. **Some devices are selected** is displayed only when a few devices in a device group are selected.

To perform a bulk edit, select the required device group check boxes and select **Activate** or **Suppress** from the **Activate** drop-down list.

If you choose to suppress alarms for a group that contains a port or device, the alarm types you specified are suppressed for that port or device even if that port or device is also in another group for which alarms are marked as **active**.

**Step 8** Click **Save and Activate**.

**Related Topics**

- What is an Alarm Policy?
- Customizing Interface Alarm Policy
- Customizing Controller Alarm Policy
- Customizing Access Point Alarm Policy
Chapter 16      Monitoring Alarms

What is an Alarm Policy?

Customizing Layer2 Switch Alarm Policy
Customizing Interface Alarm Policy
Customizing Controller Alarm Policy
Customizing Access Point Alarm Policy
Customizing Layer2 Switch Alarm Policy
Customizing Wired Infrastructure Alarm Policy
Restoring Default Settings

Viewing the Alarm Policy Summary

To view the summary of the interface, controller and access point, Layer 2 switch, and wired infrastructure alarm policies, follow these steps:

Step 1  Choose Monitor > Monitoring Tools > Alarm Policies.
Step 2  Click one of the options below to view the alarm policy summary and display a list of activated alarms on device groups:
- Interface
- Controller
- Access Point
- Layer2 Switch
- Wired Infrastructure

Restoring Default Settings

To reset the alarm policy to its default settings, follow these steps:

Step 1  Choose Monitor > Monitoring Tools > Alarm Policies.
Step 2  Select one of the alarm policy types, then click Reset to Default to restore the default settings.

The customized settings are cleared and all the alarms are activated on all devices, device groups and port groups.

Related Topics
- What is an Alarm Policy?
Getting Help for Alarms

If you receive an alarm in Monitor > Monitoring Tools > Alarms & Events for which you cannot find a resolution in the Cisco Support Community (select an alarm, then choose Troubleshoot > Support Forum), you can use Prime Infrastructure to open a support request (click an alarm, then choose Troubleshoot > Support Case). See “Troubleshooting Prime Infrastructure” in the Cisco Prime Infrastructure 3.1 Administrator Guide for more information.

Viewing Syslogs

Prime Infrastructure logs all syslogs from severity 0 through 7 (emergency through debugging messages) generated by all devices that are managed by Prime Infrastructure.

Prime Infrastructure logs and displays syslogs from managed devices only. Syslogs from devices that are not managed by Prime Infrastructure are not logged or displayed.

In order for Prime Infrastructure to provide client troubleshooting, you must configure SNMP write credentials and Telnet credentials when adding or importing the devices.

Prime Infrastructure stores a maximum of 2,000,000 syslogs with the following display limits:

- Live syslog streaming displays the latest 2,000 syslogs.
- Historic syslogs displays a maximum of 200,000 total syslogs.
- Client Troubleshooting displays the latest 1,000 syslogs.
- Infrastructure Troubleshooting displays the latest 1,000 syslogs.

Step 1
To view syslogs, choose Monitor > Monitoring Tools > Syslog Viewer. The first time you access this page, an overlay screen explains the main features.

By default, live streaming of syslogs is displayed. As syslogs are generated, they appear in the window. It might take a few seconds for data to be generated. If syslogs were generated before you clicked the Live tab, they appear in the Historic tab.

Step 2
Click the Pause icon to pause the live streaming if the incoming data is too excessive. Click the Resume arrow to resume live streaming of syslogs.

Step 3
Click Deduplicate to enable or disable deduplication of syslogs. Deduplication aggregates all syslogs of the same type into one line item and displays the count of this syslog type in the Count field.

Step 4
To troubleshoot a client based on syslogs, select one of the following options from the Troubleshooting Type drop-down menu:

- Client—Enter a client MAC address, then click Troubleshoot to start a troubleshooting session and view the syslogs for the specified client.
Viewing Syslogs

- **Infrastructure**—Select a troubleshooting option, then click **Troubleshoot**.

**Step 5** To open a TAC support case, click the **Open Support Case** icon. You need to enter your cisco.com login credentials to open a case.

**Step 6** To export the syslogs in either CSV or PDF format, click the **Export** icon.

**Step 7** Click the filter icon to view and change filter, such as location and devices. You can also enter text in the fields at the top of the table to filter the results; regular expression filtering is supported. For example, you can enter the following regular expression to filter the results:

```
^Auth, V|violation$, ^Sec*V|violation$
```

**Step 8** Click the yellow Filter icon in the Syslog Viewer page for Historic and Live tabs:

- Historic syslog page filter criteria has only location grouping. You can select either a separate group or all location with respect to the requirement. If a group is selected, then it shows syslogs from devices present in that group only.
- Live page syslog viewer filter criteria has location grouping and device grouping. Device grouping supports only 10 devices at a time and by default, the first 10 devices are selected. In the location group, unassigned devices are selected by default. You can change the preferences with respect to your requirement.

---

**Supported Syslog Formats for Event Based Inventory**

The following are the supported Syslog formats. Prime Infrastructure will trigger the inventory collection if the device syslog matches any one of the following conditions:

Message Type is any one of the following:

- LINK-3-UPDOWN
- PORT_SECURITY-6-VLAN_REMOVED
- PORT_SECURITY-6-VLAN_FULL
- G8032-STATE_IDLE
- G8032-STATE_PENDING
- G8032-STATE_PROTECTION
- G8032-STATE_FORCED_SWITCH
- G8032-STATE_MANUAL_SWITCH
- L2-G8032-3-APS_CHANNEL_INACTIVE
- L2-G8032-6-APS_CHANNEL_ACTIVE
- L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION
- L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION_CLEAR
- L2-L2VPN_ICCP_SM-3-CONFIG_LOCAL_ERROR
- L2-L2VPN_ICCP_SM-3-CONFIG_REMOTE_ERROR
- L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION
- L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION_CLEAR
- L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_FAILURE
Customizing Alarms and Events For Syslogs

You can enable Prime Infrastructure to create events for particular syslogs. You can specify a syslog message identifier, and specify the event severity and message to use when the specified syslog is received. Prime Infrastructure creates an event with the settings you specify.
Customizing Alarms and Events For Syslogs

Step 1  Choose Monitor > Monitoring Tools > Syslogs.
Step 2  Click the Historic tab.
Step 3  If there is an existing syslog for which you want to create an event, select the syslog, then click Custom Syslog Events. To create a new event for which there is not an existing syslog, click Custom Syslog Events.
Step 4  Click Add. Complete the required fields. If you selected a syslog in Step 3, the Message Type and Event Message fields are prepopulated with the values of the syslog you selected.
Step 5  Select a Default Severity level, then click OK. The Default Severity field controls the severity of the event that is created from the syslog. The syslog itself is not modified in any way.

Modifying a Customized Syslog Event

You can modify a previously created customized syslog event.

Step 1  Choose Monitor > Monitoring Tools > Syslogs.
Step 2  Click Custom Syslog Events. The Custom Syslog Events window opens displaying any previously created event mappings.
Step 3  Select the custom syslog event you want to modify, then click Edit.
Step 4  Modify the necessary fields, then click OK.

Related Topic

- Customizing Alarms and Events For Syslogs
Monitoring Clients and Users

About Wired and Wireless Clients

A client is a device that is connected to an access point or a switch. Cisco Prime Infrastructure supports both wired and wireless clients. After you add controllers and switches to Prime Infrastructure, the client discovery process starts. Wireless clients are discovered from managed controllers or autonomous access points. The controllers are polled during regular client status poll. The wireless client count includes autonomous clients as well. In the case of switches, Prime Infrastructure polls for clients immediately after the device is added and updates the device information in the database. For wired clients, the client status polling to discover client associations occurs every two hours (by default). A complete polling happens twice every day to poll complete information of all wired clients connected to all switches.

Prime Infrastructure uses background tasks to perform the data polling operations. There are three tasks associated with clients:

1. Autonomous AP Client Status
2. Lightweight Client Status
3. Wired Client Status

You can refresh the data collection tasks (such as polling interval) from the Administration > Settings > Background Tasks page.

Client status (applicable only for wired clients) is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the SNMP connection to the wired switch is lost.

For the clients of autonomous access point managed by Prime Infrastructure and for the clients authenticated using Local Extensible Authentication Protocol (LEAP), the username is not registered and is displayed as unknown.

Prime Infrastructure supports both identity and non-identity wired clients. The support for wired clients is based on the identity service. The identity service provides secure network access to users and devices and it also enables the network administrators to provision services and resources to the users based on their job functions.

Prime Infrastructure do not poll end hosts connected through VLAN 1000-1024.

Prime Infrastructure does not support VRF. Therefore, if a client is connected to a VRF-configured device, you cannot view client information.
Client Dashlets on the General Dashboard

When you log into Prime Infrastructure, the General dashboard displays a few client-related dashlets.

- Client Count By Association/Authentication—Displays the total number of clients by Association and authentication in Prime Infrastructure over the selected period of time.
  - Associated client—All clients connected regardless of whether it is authenticated or not.
  - Authenticated client—All clients connected and passed authentication, authorization and other policies, and ready to use the network.
- Client Count By Wireless/Wired—Displays the total number of wired and wireless clients in Prime Infrastructure over the selected period of time.

Related Topics
- Interactive Graphs
- Client Dashboard

Client Dashboard

The Client dashboard (Dashboard > Overview > Client) page displays the client-related dashlets. These dashlets enable you to monitor the clients on the network. The data for graphs is also polled/updated periodically and stored in Prime Infrastructure database. On the other hand, most of the information in the Client Details page are polled directly from the controller/switch.

Related Topics
- Interactive Graphs
- Adding Dashlets

Monitoring Clients and Users

Choose Monitor > Monitoring Tools > Clients and Users to view all the wired and wireless clients in your network. In addition, you can view the client association history and statistical information. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information might help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage.

Access the Client Detail page by clicking on a MAC Address to help you identify, diagnose, and resolve client issues.

Related Topics
- Filtering Clients and Users
- Viewing Clients and Users
Filtering Clients and Users

The Monitor > Monitoring Tools > Clients and Users page lists all associated clients by default. There are preset filters that allow you to view a subset of clients.

In addition, you can use the filter icon ( ) to filter the records that match the filter rules. If you want to specify a filter rule, choose All from the Show drop-down list before you click .

When you select a preset filter and click the filter icon, the filter criteria is dimmed. You can only see the filter criteria but cannot change it. When the All option is selected to view all the entries, clicking the filter icon shows the quick filter options, where you can filter the data using the filterable fields. You can also enter text in the free form text box for table filtering.

You can use the advanced search feature to narrow the client list based on specific categories and filters.

Filtering on IP Addresses

When you perform advanced client filtering on IPv6 addresses, each octet that you specify must be a complete octet. If you specify a partial octet, the filtering might not show correct results.

The following example shows how the advanced client filtering works on IPv6 addresses. This example assumes that you have the following IP addresses in the system:

10.10.40.1
10.10.40.2
10.10.40.3
10.10.240.1
Fec0::40:20
Fe80::240:20

If you search for all IP addresses containing 40, you get the following result:

10.10.40.1
10.10.40.2
10.10.40.3
Fec0::40:20

The IP addresses that contain 240 are not filtered because the filtering feature expects you to enter a complete octet.

Related Topic

• Search Methods
Viewing Clients and Users

To view complete details in the Monitor > Monitoring Tools > Clients and Users page and to perform operations such as Radio Measurement, users in User Defined groups should have the required permission before they access the Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location pages.

The following attributes are populated only when the ISE is added to Prime Infrastructure:

- ISE
- Endpoint Type
- Posture
- Authorization Profile Name

Prime Infrastructure queries the ISE for client authentication records for the last 24 hours to populate this data. If the client is connected to the network 24 hours before it is discovered in Prime Infrastructure, you might not see the ISE-related data in the table. You might see the data in client details page. To work around this, reconnect the client to the network. The ISE information is shown in the table after the next client background task run.

To view clients and users, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users to view both wired and wireless clients information. The Clients and Users page appears.

The Clients and Users table displays a few columns by default. If you want display the additional columns that are available, click ⌚ + , and then click Columns. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

**Step 2** Choose a client or user. The following information appears depending on the selected client/user.

- Client Attributes
- Client Statistics
- Client Statistics
- Client Association History
- Client Event Information
- Client Location Information
- Wired Location History
- Client CCXv5 Information

**Related Topics**

- Modifying the Clients and Users Page
- Filtering Clients and Users

**Exporting Clients and Users**

You can quickly export your clients and users list into a CSV file (spreadsheet format with comma-separated values).
When to Use the Client Troubleshooting Tool

Prime Infrastructure provides a troubleshooting tool to help you diagnose and solve issues experienced with both wired and wireless clients. This tool relies on SNMP to discover clients and collect client data. If Cisco Identity Services Engine (ISE) is integrated with Prime Infrastructure, the tool also collects ISE-based client statistics and other data shown in Prime Infrastructure’s client dashlets and reports.

Launch the client troubleshooting tool whenever you need to:

- Monitor the status of a client connection.
- Verify the current and past locations of users and their devices.
- Troubleshoot client connectivity problems.
- Troubleshoot current client issues.
- View client issue history.
- Obtain the location history for location-assisted clients.

The client troubleshooting feature is available for identity wired clients (those that are identified by ISE) and not for non-identity wired clients.

Related Topics

- Launching the Client Troubleshooting Tool
- Searching for Clients
- Analyzing Client Connection Logs
- Viewing Client Event History and Event Logs

Launching the Client Troubleshooting Tool

You can launch the Client Troubleshooting tool for any client from the Clients and Users page.

Step 1 Choose Monitor > Monitoring Tools > Clients and Users. The Clients and Users page lists all the clients the system knows (including those not currently associated).
Step 2  Click the MAC Address for the client having connection problems that you want to troubleshoot. You may find it handy to narrow the client list first, by using the Search feature. See “Troubleshooting Clients Using the Search Feature” in Related Topics.

Step 3  Click Troubleshoot and Debug.

Related Topics
- About the Client Troubleshooting Page
- How the Client Troubleshooting Tool Gives Advice
- Searching for Clients

About the Client Troubleshooting Page

The Client Troubleshooting page provides:
- Details on the current or last session for a selected wired or wireless client.
- The client’s current/last connection status, shown as a series of graphic icons.
- If connection problems are detected:
  - The nature of the connection problem (also indicated by graphic icons)
  - Advice on how to troubleshoot that problem.

Figure 17-1 shows the complete Client Troubleshooting page for a wireless client that has connected successfully. The upper Properties section of the page provides the same session details for a successfully connected client that you would see on the Clients and Users page.

Also note that, as this is a successful connection, the lower Troubleshoot section shows green check marks as the status for each stage of the wireless connection process, and provides no advice on troubleshooting the connection.

Figure 17-1  Client Troubleshooting page for Successful Wireless Client
Figure 17-2 shows the Troubleshoot section of the Client Troubleshooting page for a different wireless client (for simplicity, we have collapsed the Properties section by clicking on the section’s right arrow icon). This client had trouble connecting. As you can see, there is an alert on the 802.1X Authentication portion of the connection process and a list of steps to try to determine exactly why this was a problem.

This number and type of connection status icons, and advice in the Troubleshoot section, will vary according to the kind of client, the stage of the connection process that had problems, and the likely sources of the problem. For more information, see “How the Client Troubleshooting Tool Gives Advice” in Related Topics.
• How the Client Troubleshooting Tool Gives Advice
• Searching for Clients

How the Client Troubleshooting Tool Gives Advice

Prime Infrastructure determines the number of connection areas and the type of troubleshooting advice to present on the Client Troubleshooting page based on the stages the client passes through when establishing connection and connectivity protocols involved at each stage. Table 17-1 summarizes these stages and protocols involved at each stage.

Table 17-1 Client Connection Stages and Protocols

<table>
<thead>
<tr>
<th>Connection Stage</th>
<th>Link Connectivity</th>
<th>802.1X Authentication</th>
<th>MAC Authentication</th>
<th>Web Authentication</th>
<th>IP Connectivity</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>–</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Web Authentication</td>
<td>X</td>
<td>–</td>
<td>–</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 17-2 Details the troubleshooting advice presented for each kind of problem detected during the stages of connection building.

Table 17-2 Troubleshooting Advice for Each Connection Stage and Problem

<table>
<thead>
<tr>
<th>Client State</th>
<th>Problem</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Connectivity</td>
<td>Cannot find the client in the network</td>
<td>• Check whether the client cable is plugged into the network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client is using the proper cable to connect to the network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the port to which the client is connected is not disabled administratively.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the port to which the client is connected is not error disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the speed and duplex are set to Auto on the port to which the client is connected.</td>
</tr>
<tr>
<td>Authentication in progress</td>
<td></td>
<td>• If the client has been in this state for a long time, check the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Check whether the supplicant on the client is configured properly as required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Modify the timers related to the authentication method and try again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Use the fall back authentication feature if you are not sure which authentication method works with the client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>– Try disconnecting and reconnecting.</td>
</tr>
</tbody>
</table>
### Table 17-2  Troubleshooting Advice for Each Connection Stage and Problem (continued)

<table>
<thead>
<tr>
<th>Client State</th>
<th>Problem</th>
<th>Suggested Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Authentication</td>
<td>802.1X Authentication Failure</td>
<td>• Check whether the RADIUS server(s) is reachable from the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client choice of EAP is supported by the RADIUS server(s).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the username/password/certificate of the client is valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the certificates used by the RADIUS server are accepted by the client.</td>
</tr>
<tr>
<td>MAC Authentication</td>
<td>MAC Authentication Failure</td>
<td>• Check whether the RADIUS server(s) is reachable from the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the MAC address of the client is in the list of known clients on the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the MAC address of the client is not in the list of excluded clients.</td>
</tr>
<tr>
<td>Web Authentication</td>
<td>Client could not be authenticated through web/guest interface</td>
<td>• Check whether the guest credentials are valid and have not expired.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client can be redirected to the login page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the RADIUS server is reachable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that pop-ups are not blocked.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the DNS resolution on the client is working.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the client is not using any proxy settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the client can access https://&lt;virtual-ip&gt;/login.html</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the browser of the client accepts the self-signed certificate offered by the controller.</td>
</tr>
<tr>
<td>IP Connectivity</td>
<td>Client could not complete DHCP interaction</td>
<td>• Check whether the DHCP server is reachable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the DHCP server is configured to serve the WLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the DHCP scope is exhausted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether multiple DHCP servers are configured with overlapping scopes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check whether the local DHCP server is present. If the DHCP bridging mode is enabled (move it to second), the client is configured to get the address from the DHCP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check if the client has the static IP configured and ensure that the client generates IP traffic.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Authorization Failure</td>
<td>• Ensure that the VLAN defined for authorization is available on the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ensure that the default port ACL is configured for ACL authorization.</td>
</tr>
<tr>
<td>Successful Connection</td>
<td>None</td>
<td>None. This indicates that all previous stages were completed successfully.</td>
</tr>
</tbody>
</table>

**Related Topics**
- [Launching the Client Troubleshooting Tool](#)
Searching for Clients

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Type the full or partial client MAC address in the Advanced Search text box, and click Search. The Search Results page appears.
Step 3 Click View List to view the clients that match the search criteria in the Clients page. The Monitor > Monitoring Tools > Clients and Users page appears.
You can click the Reset link to set the table to the default display so that the search criteria is no longer applied.
Step 4 Select a client, and then click the Troubleshoot. The Troubleshooting Client page appears. If you are troubleshooting a Cisco-compatible Extension v5 client (wireless), your Troubleshooting Client page will have additional tabs.
If you receive a message that the client does not seem to be connected to any access point, you must reconnect the client and click Refresh.

Related Topics
• Launching the Client Troubleshooting Tool
• Analyzing Client Connection Logs

Analyzing Client Connection Logs

Step 1 Launch the Client Troubleshooting Tool for the client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.
Step 2 Click the Log Analysis tab to view log messages logged against the client.
Step 3 Click Start to begin capturing log messages about the client from the controller.
Step 4 Click Stop to stop log message capture.
Step 5 Click Clear to clear all log messages. Log messages are captured for ten minutes and then automatically stopped. Click Start to continue.
Step 6 Click one of the links under Select Log Messages to display log messages (the number between parentheses indicates the number of messages).

Related Topics
• Launching the Client Troubleshooting Tool
• Searching for Clients
• Viewing Client Event History and Event Logs
Viewing Client Event History and Event Logs

Step 1  Launch the Client Troubleshooting Tool. See “Launching the Client Troubleshooting Tool” in Related Topics.
Step 2  Click the **Events** tab to display the event history of a client.
Step 3  Click the **Event Log** tab to view the event log.
Step 4  Click **Start** to begin capturing log messages from the client.
Step 5  Click **Stop** when a sufficient number of messages have been collected.

The Client Troubleshooting Event log and Messaging features are available to CCX Version 6 clients only if the Management Service version is 2 and later.

Related Topics
- Launching the Client Troubleshooting Tool
- Searching for Clients

Checking Client ISE Authentication History and Identity Services

Step 1  Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.
Step 2  Click the **Identity Services Engine** tab to view information about ISE authentication.
Step 3  Enter the date and time ranges to retrieve historical authentication and authorization information, and then click **Submit**. The results of the query are displayed in the Authentication Records portion of the page.
Step 4  Click the **Identity Services Engine** tab to view information about the identity services parameters. You must configure the Identity Services Engine (ISE) before you access this tab.

If the ISE is not configured, it provides a link to add an ISE to Prime Infrastructure. The ISE provides authentication records to Prime Infrastructure via REST API. The network administrator can choose a time period for retrieving authentication records from the ISE.

Related Topics
- Launching the Client Troubleshooting Tool
- Searching for Clients
- Checking Client Clean Air Environment
Checking Client Clean Air Environment

Step 1  Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2  Click the CleanAir tab to view information about the air quality parameters and active interferer for the CleanAir-enabled access point.

Step 3  Click CleanAir Details to know more about the air quality index.

Related Topics
- Launching the Client Troubleshooting Tool
- Searching for Clients

Running Diagnostic Tests on Problem Clients

Step 1  Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2  (Optional) Click the Test Analysis tab if Cisco-compatible Extension Version 5 or Version 6 clients are available.

Step 3  Check the check box for the applicable diagnostic test, enter any appropriate input information, and click Start. The Test Analysis tab allows you to run a variety of diagnostic tests on the client.

Related Topics
- Launching the Client Troubleshooting Tool
- Searching for Clients
- When to Run Diagnostic Tests on Problem Clients

When to Run Diagnostic Tests on Problem Clients

Before you begin, ensure that you have reviewed the test qualifications and restrictions. See Related Topics.

The following diagnostic tests are available on the Test Analysis tab:
- DHCP—Executes a complete DHCP Discover/Offer/Request/ACK exchange to determine that the DHCP is operating properly between the controller and client.
- IP Connectivity—Causes the client to execute a ping test of the default gateway obtained in the DHCP test to verify that IP connectivity exists on the local subnet.
- DNS Ping—Causes the client to execute a ping test of the DNS server obtained in the DHCP test to verify that IP connectivity exists to the DNS server.
Chapter 17  Monitoring Clients and Users

Pinging Problem Clients with Text Messages

Step 1  Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2  (Optional) For Cisco-compatible Extension Version 5 or Version 6 clients, a Messaging tab will appear which can be used to send an instant text message to the user of this client. From the Message Category drop-down list, choose a message, and click Send.

Related Topics

- Launching the Client Troubleshooting Tool
- Searching for Clients
- Running Diagnostic Tests on Problem Clients

Viewing Real Time Troubleshooting (RTTS) Details

Step 1  Launch the Client Troubleshooting Tool for the Client you want to analyze. See “Launching the Client Troubleshooting Tool” in Related Topics.

Step 2  Click the RTTS tab to view the Real Time Troubleshooting (RTTS) details.

Step 3  Select modules to debug and debug level.

Step 4  Click Run. The RTTS manager executes a set of commands in the controllers connected to the client based on the selected debug modules and debug level and displays the RTTS details.

Related Topics

- Launching the Client Troubleshooting Tool
- Running Diagnostic Tests on Problem Clients
- When to Run Diagnostic Tests on Problem Clients

- DNS Resolution—Causes the DNS client to attempt to resolve a network name known to be resolvable to verify that name resolution is functioning correctly.
- 802.11 Association—Directs an association to be completed with a specific access point to verify that the client is able to associate properly with a designated WLAN.
- 802.1X Authentication—Directs an association and 802.1X authentication to be completed with a specific access point to verify that the client is able to properly complete an 802.1x authentication.
- Profile Redirect—At any time, the diagnostic system might direct the client to activate one of the configured WLAN profiles and to continue operation under that profile.

To run the profile diagnostic test, the client must be on the diagnostic channel. This test uses the profile number as the input. To indicate a wildcard redirect, enter 0. With this redirect, the client is asked to disassociate from the diagnostic channel and associate with any profile. You can also enter a valid profile ID. Because the client is on the diagnostic channel when the test is run, only one profile is returned in the profile list. You should use this profile ID in the profile redirect test (when wildcard redirecting is not desired).

Related Topics

- Launching the Client Troubleshooting Tool
- Searching for Clients
- Running Diagnostic Tests on Problem Clients
Step 5  Click the Filter tab to filter the RTTS details based on debug time, controller name, controller IP, severity, and debug message.

Step 6  Click the Export tab to export the debug details as a csv file.

You can also debug other controllers based on the selected debug modules and debug levels by using the Choose different controllers option.

The RTTS Manager supports five concurrent RTTS debug sessions and each debug session is limited to five devices.

Related Topics
- Launching the Client Troubleshooting Tool
- Debug Commands for RTTS

Debug Commands for RTTS

Table 17-3 contains the list of debug commands for Legacy controllers and Converged Access Controllers 5760/3850/3650 Wireless LAN Controllers (WLCs).

<table>
<thead>
<tr>
<th>Controller</th>
<th>Modules to Debug</th>
<th>Debug Level</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy</td>
<td>All</td>
<td>Debug Level</td>
<td>debug capwap info enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug dot1x all enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug mobility directory enable</td>
</tr>
<tr>
<td>Dot1.x</td>
<td>Detail</td>
<td>debug dot1x all enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td>debug dot1x events enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High Level</td>
<td>debug dot1x states enable</td>
<td></td>
</tr>
<tr>
<td>Legacy</td>
<td>Mobility</td>
<td>debug mobility packet enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detail</td>
<td>debug mobility keepalive enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td>debug mobility directory enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High Level</td>
<td>debug mobility handoff enable</td>
<td></td>
</tr>
<tr>
<td>Wireless Client Join</td>
<td>Detail</td>
<td>debug client &lt;macAddress&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td>debug client &lt;macAddress&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High Level</td>
<td>debug client &lt;macAddress&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Related Topic

- Launching the Client Troubleshooting Tool

### Tracking Clients

This feature enables you to track clients and be notified when they connect to a network.

**Step 1**
Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2**
Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.

This table supports a maximum of 2000 rows. To add or import new rows, you must first remove some older entries.

**Step 3**
Click Add to track a single client, and then enter the following parameters:

---

### Table 17-3 List of Debug Commands for Legacy Controllers and NGWC Controllers

<table>
<thead>
<tr>
<th>Controller</th>
<th>Modules to Debug</th>
<th>Debug Level</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGWC</td>
<td>All</td>
<td>Debug</td>
<td>debug capwap ap error</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug dot1x events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug capwap ios detail</td>
</tr>
<tr>
<td></td>
<td>Dot1.x</td>
<td>Detail</td>
<td>debug wcm-dot1x detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug wcm-dot1x all</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug dot1x all</td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td></td>
<td>debug wcm-dot1x errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug dot1x errors</td>
</tr>
<tr>
<td></td>
<td>High Level</td>
<td></td>
<td>debug wcm-dot1x trace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug wcm-dot1x event</td>
</tr>
<tr>
<td></td>
<td>Mobility</td>
<td>Detail</td>
<td>debug mobility all</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug mobility error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Level</td>
<td>debug mobility handoff</td>
</tr>
<tr>
<td></td>
<td>Wireless Client</td>
<td>Detail</td>
<td>debug wcdb error</td>
</tr>
<tr>
<td></td>
<td>Join</td>
<td></td>
<td>debug wcdb event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug wcdb db</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug ip dhcp snooping events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug ip dhcp server events</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td></td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Level</td>
<td>debug client mac &lt;macAddress&gt;</td>
</tr>
</tbody>
</table>
Tracking Multiple Clients

This feature enables you to track multiple clients and be notified when they connect to a network.

Step 1  Choose Monitor > Monitoring Tools > Clients and Users.

Step 2  Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.

Step 3  Click Add to track a single client, and then enter the following parameters:
- Client MAC address
- Expiration—Choose Never or enter a date.

Step 4  If you have a long list of clients, click Import to track multiple clients. This allows you to import a client list from a CSV file. Enter the MAC address and username.

A sample CSV file can be downloaded that provides data format:

# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never

A maximum of 2000 clients can be tracked. If you have reached the limit, you will have to remove some clients from the list before you can add more.

Related Topics
- Launching the Client Troubleshooting Tool
- Specifying Notification Settings

Specifying Notification Settings

Step 1  Choose Monitor > Monitoring Tools > Clients and Users.

Step 2  Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.

Step 3  Select the tracked client(s) for which you want to specify notification settings.

Step 4  Select a notification settings option from the following:
• Purged Expired Entries—You can set the duration to keep tracked clients in Prime Infrastructure database. Clients can be purged as follows:
  – after 1 week
  – after 2 weeks
  – after 1 month
  – after 2 months
  – after 6 months
  – kept indefinitely
• Notification Frequency—You can specify when Prime Infrastructure sends a notification of a tracked client:
  – on first detection
  – on every detection
• Notification Method—You can specify that the tracked client event generates an alarm or sends an email message.

Step 5  Enter the email address.
Step 6  Click Save.

Related Topics
• Tracking Clients
• Identifying Unknown Users

When to Assign a Username

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administrator can assign a username to a device.
If a client device is authenticated to the network through web auth, Prime Infrastructure might not have username information for the client (applicable only for wired clients).
Clients are marked as unknown when the NMSP connection to the wired switch is lost. A client status (applicable only for wired client) is noted as connected, disconnected, or unknown:
• Connected clients—Clients that are active and connected to a wired switch.
• Disconnected clients—Clients that are disconnected from the wired switch.
• Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost.

Related Topics
• Identifying Unknown Users
Identifying Unknown Users

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Click Identify Unknown Users.
Step 3 Click Add to add a user.
Step 4 Enter the MAC address and username and click Add.
   Once a username and MAC address have been added, Prime Infrastructure uses this data for client lookup by matching the MAC address.
Step 5 Repeat Step 3 to Step 4 to enter a MAC Address and its corresponding username for each client.
Step 6 Click Save.
   The username is updated only when the next association of the client occurs.
   This table supports a maximum of 10,000 rows. To add or import new rows, you must first remove some older entries.

Related Topics
- When to Assign a Username
- Tracking Clients
- Modifying the Clients and Users Page

Modifying the Clients and Users Page

You can add, remove, or reorder columns in the Clients table.

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Click the settings icon, then click Columns.
Step 3 Select the columns to show
Step 4 Click Reset to restore the default view.
Step 5 Click Close to confirm the changes.

Related Topics
- Tracking Clients
- Enabling Automatic Client Troubleshooting

Enabling Automatic Client Troubleshooting

In the Settings > Client page, you can enable automatic client troubleshooting on a diagnostic channel. This feature is available only for Cisco-compatible Extension clients Version 5.
To enable automatic client troubleshooting, follow these steps:

**Step 1** Choose **Administration > Settings > System Settings**.

**Step 2** From the left sidebar menu, choose **Client**.

**Step 3** Check the **Automatically troubleshoot client on diagnostic channel** check box.

When the check box is selected, Prime Infrastructure processes the diagnostic association trap. When it is not selected, Prime Infrastructure raises the trap, but automated troubleshooting is not initiated.

**Step 4** Click **Save**.

---

**Related Topics**
- Modifying the Clients and Users Page
- Obtaining Radio Measurements for a Client

---

### When to Obtain Radio Measurements for a Client

In the client page, you can obtain radio measurements only if the client is Cisco-compatible Extensions v2 (or higher) and in the associated state (with a valid IP address). If the client is busy when asked to do the measurement, it determines whether to honor the measurement or not. If it declines to make the measurement, it shows no data from the client.

This feature is available to CCX Version 6 clients only if the Foundation service version is 1 or later.

**Related Topic**
- Obtaining Radio Measurements for a Client

---

### Obtaining Radio Measurements for a Client

To receive radio measurements, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Clients and Users**.

**Step 2** Click the circle next to a client.

You can also perform a search for a specific client using Prime Infrastructure Search feature. See “Searching for Clients” in Related Topics.

**Step 3** From the **Test** drop-down list, choose **Radio Measurement**.

The Radio Measurement option only appears if the client is Cisco-compatible Extensions v2 (or higher) and is in the associated state (with a valid IP address).

**Step 4** Check the check box to indicate if you want to specify beacon measurement, frame measurement, channel load, or noise histogram.

Click **Initiate**. The different measurements produce differing results. See “Radio Measurement Results for a Client” in Related Topics.
The measurements take about 5 milliseconds to perform. A message from Prime Infrastructure indicates the progress. If the client chooses not to perform the measurement, that is communicated.

Related Topics
- Searching for Clients
- When to Obtain Radio Measurements for a Client
- Radio Measurement Results for a Client

Radio Measurement Results for a Client

Depending on the measurement type requested, the following information might appear:

- **Beacon Response**
  - Channel—The channel number for this measurement
  - BSSID—6-byte BSSID of the station that sent the beacon or probe response
  - PHY—Physical Medium Type (FH, DSS, OFDM, high rate DSS or ERP)
  - Received Signal Power—The strength of the beacon or probe response frame in dBm
  - Parent TSF—The lower 4 bytes of serving access point TSF value
  - Target TSF—The 8-byte TSF value contained in the beacon or probe response
  - Beacon Interval—The 2-byte beacon interval in the received beacon or probe response
  - Capability information—As found in the beacon or probe response

- **Frame Measurement**
  - Channel—Channel number for this measurement
  - BSSID—BSSID contained in the MAC header of the data frames received
  - Number of frames—Number of frames received from the transmit address
  - Received Signal Power—The signal strength of 802.11 frames in dBm

- **Channel Load**
  - Channel—The channel number for this measurement
  - CCA busy fraction—The fractional duration over which CCA indicated the channel was busy during the measurement duration defined as ceiling (255 times the duration the CCA indicated channel was busy divided by measurement duration)

- **Noise Histogram**
  - Channel—The channel number for this measurement
  - RPI density in each of the eight power ranges

Related Topics
- When to Obtain Radio Measurements for a Client
- Obtaining Radio Measurements for a Client
Viewing Client V5 Statistics

To access the Statistics request page, follow these steps:

**Step 1**  Choose "Monitor > Monitoring Tools > Clients and Users."

**Step 2**  Select a client.

**Step 3**  From the Test drop-down list, choose V5 Statistics.

This menu is shown only for CCX v5 and later clients.

**Step 4**  Click Go.

**Step 5**  Select the desired type of stats (Dot11 Measurement or Security Measurement).

**Step 6**  Click Initiate to initiate the measurements.

The duration of measurement is five seconds.

**Step 7**  Depending on the V5 Statistics request type, the following counters are displayed in the results page:

- **Dot11 Measurement**
  - Transmitted Fragment Count
  - Multicast Transmitted Frame Count
  - Failed Count
  - Retry Count
  - Multiple Retry Count
  - Frame Duplicate Count
  - Rts Success Count
  - Rts Failure Count
  - Ack Failure Count
  - Received Fragment Count
  - Multicast Received Frame Count
  - FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.
  - Transmitted Frame Count

- **Security**
  - Pairwise Cipher
  - Tkip ICV Errors
  - Tkip Local Mic Failures
  - Tkip Replays
  - Ccmp Replays
  - Ccmp Decryp Errors
  - Mgmt Stats Tkip ICV Errors
  - Mgmt Stats Tkip Local Mic Failures
  - Mgmt Stats Tkip Replays
  - Mgmt Stats Ccmp Replays
Viewing Client Operational Parameters

To view specific client operational parameters, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Clients and Users**.

**Step 2** Select a client.

**Step 3** From the **Test** drop-down list, choose **Operational Parameters**.

The following information is displayed:

**Operational Parameters:**

- **Device Name**—User-defined name for device.
- **Client Type**—Client type can be any of the following:
  - laptop(0)
  - pc(1)
  - pda(2)
  - dot11mobilephone(3)
  - dualmodephone(4)
  - wgb(5)
  - scanner(6)
  - tabletpc(7)
  - printer(8)
  - projector(9)
  - videoconfsystem(10)
  - camera(11)
  - gamingsystem(12)
  - dot11deskphone(13)
  - cashregister(14)
  - radiotag(15)
- rfidsensor(16)
- server(17)

- SSID—SSID being used by the client.
- IP Address Mode—The IP address mode such as static configuration or DHCP.
- IPv4 Address—IPv4 address assigned to the client.
- IPv4 Subnet Address—IPv4 subnet address assigned to the client.
- IPv6 Address—IPv6 address assigned to the client.
- IPv6 Subnet Address—IPv6 address assigned to the client.
- Default Gateway—The default gateway chosen for the client.
- Operating System—Identifies the operating system that is using the wireless network adapter.
- Operating System Version—Identifies the version of the operating system that is using the wireless network adapter.
- WNA Firmware Version—Version of the firmware currently installed on the client.
- Driver Version—
- Enterprise Phone Number—Enterprise phone number for the client.
- Cell Phone Number—Cell phone number for the client.
- Power Save Mode—Displays any of the following power save modes: awake, normal, or maxPower.
- System Name—
- Localization—

Radio Information:
- Radio Type—The following radio types are available:
  - unused(0)
  - fhss(1)
  - dsss(2)
  - irbaseband(3)
  - ofdm(4)
  - hrdss(5)
  - erp(6)
- Radio Channel—Radio channel in use.

DNS/WNS Information:
- DNS Servers—IP address for DNS server.
- WNS Servers—IP address for WNS server.

Security Information:
- Credential Type—Indicates how the credentials are configured for the client.
- Authentication Method—Method of authentication used by the client.
- EAP Method—Method of Extensible Authentication Protocol (EAP) used by the client.
- Encryption Method—Encryption method used by the client.
Viewing Client Profiles

To view specific client profile information, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Select a client.

**Step 3** From the More drop-down list, choose Profiles.

The following information is displayed:

- Profile Name—List of profile names as hyperlinks. Click a hyperlink to display the profile details.
- SSID—SSID of the WLAN to which the client is associated.

Disabling Current Clients

To disable a current client, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Select a client.

**Step 3** Click Disable. The Disable Client page appears.

**Step 4** Enter a description in the Description text box.

**Step 5** Click OK.

Once a client is disabled, it cannot join any network/ssid on controller(s). To enable the client again, choose Configuration > Network > Network Devices > Wireless Controller > Device Name > Security > Manually Disabled Clients, and remove the client entry.
Removing Current Clients

To remove a current client, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Select a client.

**Step 3** Choose Remove.

**Step 4** Click Remove to confirm the deletion.

---

**Related Topic**

- Enabling Mirror Mode

---

Enabling Mirror Mode

When a client is enabled, mirror mode enables you to duplicate (to another port) all the traffic originating from or terminating at a single client device or access point.

Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port because any connections to this port become unresponsive.

To enable mirror mode, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Select a client.

**Step 3** From the More drop-down list, choose Enable Mirror Mode.

**Step 4** Click Go.

---

**Related Topics**

- Mapping Recent Client Locations

---

Mapping Recent Client Locations

**Note**

Cisco MSE is not required to be managed in Cisco Prime Infrastructure for Recent Map to work.

To display a high-resolution map of the client recent location, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Choose a client from the Client Username column.

**Step 3** From the More drop-down list, choose Recent Map (High Resolution).
Step 4  Click Go.

---

**Related Topic**
- Mapping Current Client Locations

### Mapping Current Client Locations

*Note*
Cisco MSE is not required to be managed in Cisco Prime Infrastructure for Present Map to work.

To display a high-resolution map of the client current location, follow these steps:

**Step 1**  Choose **Monitor > Monitoring Tools > Clients and Users**.
**Step 2**  Select a client.
**Step 3**  From the **More** drop-down list, choose **Present Map (High Resolution)**.
**Step 4**  Click Go.

---

**Related Topic**
- Running Client Sessions Reports

### Running Client Sessions Reports

To view the most recent client session report results for a client, follow these steps:

**Step 1**  Choose **Monitor > Monitoring Tools > Clients and Users**.
**Step 2**  Select a client.
**Step 3**  From the **More** drop-down list, choose **Client Sessions Report**.
**Step 4**  Click Go. The Client Session report details display.

---

**Related Topic**
- Viewing Client Roam Reason Reports

### Viewing Client Roam Reason Reports

To view the most recent roam report for this client, follow these steps:

**Step 1**  Choose **Monitor > Monitoring Tools > Clients and Users**.
**Step 2** Select a client.

**Step 3** From the More drop-down list, choose **Roam Reason**.

**Step 4** Click **Go**.

This page displays the most recent roam report for the client. Each roam report has the following information:

- New AP MAC address
- Old (previous) AP MAC address
- Previous AP SSID
- Previous AP channel
- Transition time—Time that it took the client to associate to a new access point.
- Roam reason—Reason for the client roam.

**Related Topic**
- Viewing Detecting Access Point Details

---

**Viewing Detecting Access Point Details**

To display details of access points that can hear the client including the signal strength/SNR, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Clients and Users**.

**Step 2** Select a client.

**Step 3** From the **More** drop-down list, choose **Detecting APs**.

**Step 4** Click **Go**.

**Related Topic**
- Viewing Client Location History

---

**Viewing Client Location History**

To display the history of the client location based on RF fingerprinting, follow these steps:

**Step 1** Choose **Monitor > Monitoring Tools > Clients and Users**.

**Step 2** Select a client.

**Step 3** From the **More** drop-down list, choose **Location History**.

**Step 4** Click **Go**.
### Related Topic
- [Viewing Voice Metrics for a Client](#)

---

## Viewing Voice Metrics for a Client

To view traffic stream metrics for this client, follow these steps:

**Step 1** Choose Monitor > Monitoring Tools > Clients and Users.

**Step 2** Select a client.

**Step 3** From the More drop-down list, choose Voice Metrics.

**Step 4** Click Go.

The following information appears:

- **Time**—Time that the statistics were gathered from the access point(s).
- **QoS**
- **AP Ethernet MAC**
- **Radio**
- **% PLR (Downlink)**—Percentage of packets lost on the downlink (access point to client) during the 90 second interval.
- **% PLR (Uplink)**—Percentage of packets lost on the uplink (client to access point) during the 90 second interval.
- **Avg Queuing Delay (ms) (Uplink)**—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed.
- **% Packets > 40 ms Queuing Delay (Downlink)**—Percentage of queuing delay packets greater than 40 ms.
- **% Packets 20ms—40ms Queuing Delay (Downlink)**—Percentage of queuing delay packets greater than 20 ms.
- **Roaming Delay**—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.

---

### Related Topic
- [Viewing Client Location History](#)
Performance Routing Version 3 Based Network Monitoring

Performance Routing

Performance Routing Version 3 (PfRv3) represents the third generation of enhancement to the intelligent path control capabilities offered by Cisco. PfR monitors network performance and selects the best path for each application based upon advanced criteria such as reachability, delay, jitter and packet loss. PfR can evenly distribute traffic to maintain equivalent link utilization levels using an advanced load balancing technique.

PfRv3 is an intelligent path control of the IWAN initiative and provides a business-class WAN over Internet transports. PfR allows customers to protect critical applications from fluctuating WAN performance while intelligently load balancing traffic over all WAN paths.

PfR comprises two major Cisco IOS components:

- Master Controller—The master controller is a policy decision point at which policies are defined and applied to various traffic classes that traverse the border router systems. The master controller can be configured to learn and control traffic classes on the network.
- Border Routers (BR)— The border routers are in the data forwarding path. The border router collects data from the Performance Monitor cache and from the smart probe results. The border router influences the packet forwarding path as directed by the master controller to manage user traffic.

Getting Access to PfR Monitoring for a User Group

PfR monitoring is enabled for the Prime Infrastructure root user group by default.

To access the PfR monitoring landing page by other user groups, do the following:

Step 1 Choose Administration > User, Roles & AAA > User.
Step 2 Click Users in the left pane, and choose Select a command > Add User, then click Go.
Step 3 Enter the username and password, and then confirm the password, for the new user.
Step 4 Assign user group to the new user by selecting the check box next to each user group which has PfR Monitoring Access entry in its task list.
Step 5 Click Save.
Step 6  Log in to Prime Infrastructure using the new Username and Password.

Step 7  Choose Services > Application Visibility & Control > PfR Monitoring.

Step 8  If you do not see PfR Monitoring, go to Administration > User, Roles & AAA > User Groups.

Step 9  Click Task List corresponding to the assigned user group and check whether PfR Monitoring is available.

Step 10 If PfR Monitoring is not available in the task list, click the Task Permissions tab and check the PfR Monitoring Access check box under the Network Monitoring list.

Step 11  Click Submit.

PfR Monitoring Page

You can launch the PfR monitoring page by choosing Services > Application Visibility & Control > PfR Monitoring. The PfR monitoring page has PfR Events tab including Site to Site PfR Events table, a filter panel, Metrics panel (Service Provider view and Differentiated Services Code Point (DSCP) View charts), time slider, and Compare WAN Links tab.

You can perform the following tasks in the PfR monitoring page:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh the page</td>
<td>Click the Refresh icon 🔄 at the top right corner of the PfR monitoring page, to manually refresh the PfR landing page.</td>
</tr>
</tbody>
</table>
| Changing Settings            | Click the settings icon at the top right corner of the PfR monitoring page. The PfR Settings pop-up window will appear.
You can select your preferences for the following:
• Global settings > Virtual Routing Forwarding (VRF).
• PfR Events tab
• Site to Site tab
• Compare WAN Links tab
To enable advanced troubleshooting settings, contact Cisco support. |
| View in-line help            | Click the info icon ❌ at the top right corner of the PfR monitoring page, to view the in-line help for the respective page. |
| View live topology           | Click the topology icon ⚫ next to any site pair to view the live topology that shows traffic corresponding to different DSCPs. For more information see Viewing Site to Site PfR Topology. Choose the VRF for which you want to see the topology, from the VRF drop-down list. The VRFs listed corresponds to the site pair you have chosen. |
| View border router or link metrics | Click a link or border router in the Live topology to view the metrics details at the bottom. |
Site to Site PfR Events Table

The Site to Site PfR events table displays sites (Hub, Branch and Transit sites) and the events including Threshold Crossing Alert (TCA), Route change (RC) and Immitigable event (IME). The PfR events that occurred over last 72 hours are displayed, by default.

The events are represented by red and blue dots in the Site to Site PfR events table. The metric violations that could not be corrected by the PfR are classified as IME and indicated as red dots in the table. The degraded network performance that are identified and corrected by PfR are indicated by blue dots.

The events in the table are sorted such that the site combinations with maximum number of IMEs, is present at top row of the table. If two site combinations have equal number of IMEs, then the one with maximum number of events (including IME, TCA, and RC) is placed on the top of the table and indicated in red color. You can view the site hierarchy by hovering the mouse over the source and destination sites.

Related Topics

- PfR Monitoring Page
- PfR Filter Panel
- Viewing Site to Site PfR Topology
- Time Slider

PfR Filter Panel

The PfR Filter Panel allows you to filter the events based on various filters listed in the Table 18-1. The Metrics panel and the Site to Site PfR Events table display the details based on the selected filter options.
You can view the selected filter options in the top of the filter panel. You can click more to view all the selected filter options.

**Related Topics**
- PfR Monitoring Page
- Site to Site PfR Events Table
- Time Slider

### Service Provider View and DSCP View Charts

The Metrics panel displays Service provider View and DSCP View charts.

Service Provider View Chart—Displays the metrics gathered using the TCA. Each service provider is represented by a unique color in the chart. The charts available in this view are:
- Unreachability event count over time
- Maximum Delay over time
- Maximum Jitter over time
- Maximum Packet Loss% over time
DSCP View Chart—Displays six different metric charts with respect to different DSCPs. A maximum of five DSCPs can be viewed in the maximized view of the chart. You can also choose the required DSCP using the DSCP filter. The charts available in this view are:

- Service Provider (SP) Bandwidth (B/W) usage per DSCP
- DSCP vs TCAs
- DSCP vs Unreachable TCAs
- Maximum Delay Over time
- Maximum Jitter Over time
- Maximum Packet Loss% Over time

You can perform the following tasks in the Metrics Panel:

- Viewing different charts—Click the arrow icons in the metrics panel.
- Adding new charts—Click the add icon. In the Add components dialog box, choose the required components and click Save.

### Related Topics

- PfR Monitoring Page
- Site to Site PfR Events Table
- Time Slider

### Time Slider

A time slider present at the bottom of the page, represents the time range selected using the filter. You can drag the slider and set a particular time range. The Metrics Panels and the Site to Site PfR events table change corresponding to the set time range.

### Related Topics

- PfR Monitoring Page
- Viewing Site to Site PfR Topology
- Service Provider View and DSCP View Charts
- Site to Site PfR Events Table

### Viewing Site to Site PfR Topology

From the Services > Application Visibility & Control > PfR Monitoring page, you can view various Site-to Site details as described in Table 18-3.
### Table 18-3  Site to Site Topology Tasks

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View detailed information about Site to Site events</td>
<td>Click a dot in the Site to Site events table. You can see a Site to Site pop-up window. The pop-up window displays the type of events occurred in the selected time range, along with the event details in a table format. The violated metrics (Byte Lost%, Delay, Jitter, Packet Loss%) that cause IME are indicated within Square Brackets [].</td>
</tr>
</tbody>
</table>
| View Site to Site topology                 | Click Site to Site details in the pop-up window to view the schematic Site to Site topology representation and All Events table including the details of all events. The topology includes legends representing border router, master controller, service provider, and Internal and External links. The topology is plotted based on the data for a minimum of 72 hours, even if you select a time frame of less than 72 hours using the time filter. The Border router and the corresponding links are dimmed and you cannot click them for the following reasons:  
  - If the inventory collection has failed for the border router.  
  - If the border router is not managed.  
  - If you are not authorized to access the border router (as per Role Based Access Control). Choose the VRF for which you want to see the topology, from the VRF drop-down list. |
| View device metrics                        | Click a border router or Master controller in the topology to view the device metrics pop-up window. You can also click Launch Device Dashboard in the device metrics pop-up window to view the Device dashlets in the Performance dashboard. See Performance Dashboard in Related Topics. |
| View device details                        | Click Analyze in the device metrics pop-up window to view the device context tab. You can see:  
  - Border router Metrics—Displays three charts in which the utilization of service provider Bandwidth, memory and CPU are plotted for the selected time range, and a chart in which Service Provider Usage is plotted against Traffic. Click the zoom icon to see the enlarged view of the chart. You can further enlarge the chart to view the data pattern in a specific time interval by moving the slider.  
  - WAN Link Usage and Performance—Displays a table that shows WAN link usage and performance with respect to DSCP markings, for the WAN interfaces of the selected border router. The data includes Egress Bandwidth (B/W) usage, number of TCAs, RCs and IMEs occurred and the number of applications associated to DSCP markings. The number of applications is visible only if AVC NetFlow is received by Prime Infrastructure for this WAN link.  
  - Click the Expand arrow adjacent to the DSCP to drill-down to further details. |
Comparing WAN Interfaces

The Compare WAN Links tab shows a guided workflow for comparing the WAN link usage and performance of the selected WAN links.

Step 1 Choose Services > Application Visibility & Control > PfR Monitoring.
Step 2 Click Compare WAN Links tab.

Table 18-3 Site to Site Topology Tasks (continued)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Link Metrics</td>
<td>Click an egress or ingress link in the topology, to view a Link Metrics pop-up window. You can click Launch Interface Dashboard in the Link Metrics pop-up window to view the Interface dashlets in the Performance dashboard.</td>
</tr>
<tr>
<td>View link details</td>
<td>Click Analyze in the Link Metrics pop-up window to view the link context tab. You can see:</td>
</tr>
<tr>
<td></td>
<td>• WAN Link Metrics—Displays SP Usage Trend, Top 10 Application Traffic (In and Out), Top 10 Application Usage (Out), Top QOS Class Map Statistics Trend, SP Usage - Traffic between Source Site and All Sites, and Interface Availability Trend charts.</td>
</tr>
<tr>
<td></td>
<td>• WAN Link Usage and Performance—Displays a table that shows WAN Link Usage and Performance with respect to DSCP markings, for the WAN interface.</td>
</tr>
<tr>
<td></td>
<td>• Click the Expand arrow adjacent to the DSCP to drill-down to further details.</td>
</tr>
</tbody>
</table>

Troubleshooting the Topology Diagram

If the topology is not loaded, check the following:

• Availability of any one of the border router, master controller or service provider.
• Availability of PfR Bandwidth between the sites for the selected time Interval.
• There is no inventory failure in the protocol endpoint.
• The Interfaces are managed by Prime Infrastructure.
• Availability of WAN links.
• Whether you have logged in as root user and have access to the required devices.

Related Topics

• PfR Monitoring Page
• Comparing WAN Interfaces
• Performance Dashboards
• Viewing Site to Site PfR Topology

Comparing WAN Interfaces

The Compare WAN Links tab shows a guided workflow for comparing the WAN link usage and performance of the selected WAN links.
### Chapter 18      Performance Routine Version 3 Based Network Monitoring

#### Comparing WAN Interfaces

**Step 3** Click the filter icon to view the Time Filter, if required.

**Step 4** Choose the required options from **PfR Controlled Site, Border Router** and **WAN Interface/SP** drop-down lists, in each WAN link you want to compare.

**Step 5** Click **Compare** to compare the selected WAN links.

**Step 6** If you want to add third WAN link for comparison click + icon and select the required options and click **Update**.

**Step 7** Click the edit icon to change the previous selections.

You can view charts representing WAN link Utilization, Top N application, Top QOS Trend and Interface Availability of the select WAN links, and a table that compares the Egress Bandwidth (B/W) usage, number of TCAs, RCs and IMEs occurred and number of applications routed, for the selected WAN links.

**Step 8** Click the required WAN link metrics to view the respective charts.

---

You can also click **Compare WAN Links** in the device metrics pop-up window in the or click **Add To Compare** in the **Link Metrics** pop-up window to view the **Compare WAN Links** tab. The border router and WAN Interface details get automatically populated based on the device or link you clicked.

**Related Topics**
- PfR Monitoring Page
- Viewing Site to Site PfR Topology
Monitoring Wireless Technologies

This chapter contains the following sections:

- Monitoring Radio Resource Management
- Monitoring Interferers
- Monitoring Media Streams
- Troubleshooting Unjoined Access Points
- Monitoring Chokepoints
- Monitoring WiFi TDOA Receivers

Monitoring Radio Resource Management

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points to automatically discover rogue access points.

RRM, built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment.

Prime Infrastructure would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into Prime Infrastructure events as informational and were maintained by the event dispatcher. The reason behind the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load, and the like) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

RRM statistics help to identify trouble spots and provide possible reasons for channel or power-level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on event groupings. The event groupings may include the following:

- Worst performing access points
- Configuration mismatch between controllers in the same RF group
- Coverage holes that were detected by access points based on threshold
- Precoverage holes that were detected by controllers
- Ratios of access points operating at maximum power

Note

RRM dashboard information is available only for lightweight access points.
Channel Change Notifications

Notifications are sent to the Prime Infrastructure RRM dashboard when a channel change occurs. Channel changes depend on the Dynamic Channel Assignment (DCA) configuration where the mode can be set to auto or on demand. When the mode is auto, channel assignment is periodically updated for all lightweight access points that permit this operation. When the mode is set to on demand, channel assignments are updated based on request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global defaults.

When a channel change trap is received after an earlier channel change, the event is marked as Channel Revised; otherwise, it is marked as Channel Changed. A channel change event can have multiple causes. The reason code is factored and equated to 1, irrespective of the number of reasons that are possible. For example, suppose a channel change might be caused by signal, interference, or noise. The reason code in the notification is refactored across the reasons. If the event had three causes, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events have the same reason code, all three reasons are equally factored to determine the cause of the channel change.

Transmission Power Change Notifications

Notifications are sent to the Prime Infrastructure RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one, irrespective of the number of reasons for the event to occur.

RF Grouping Notifications

When RRM is run on the controller, dynamic grouping is done and a new group leader is chosen. Dynamic grouping has three modes: Automatic, Off, and Leader. When grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With automatic grouping, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

RRM Dashboard

The RRM dashboard is available at Monitor > Wireless Technologies > Radio Resource Management.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups. To get the latest number of RF Groups, run the configuration synchronization background task.
- The RRM Statistics portion shows network-wide statistics.
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
  - Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio(s) improved the channel plan of the system as evaluated by the algorithm.
  - WiFi Interference
- Load
- Radar
- Noise
- Persistent Non-WiFi Interference
- Major Air Quality Event
- Other

- The Channel Change shows all events complete with causes and reasons.
- The Configuration Mismatch portion shows comparisons between leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour period.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups (derived from all of the controllers which are currently managed by Prime Infrastructure).
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the preset value.

Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.

- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

- Channel Change - APs with channel changes—Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.

- Coverage Hole - APs reporting coverage holes—The top five access points filtered by IF Type 11a/n which triggered a coverage hole event (threshold based) are displayed.

- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.
This maximum power portion shows the values from the last 24 hours and is poll driven. This occurs every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n lightweight access points which have been operating at maximum power.

This maximum power portion shows the value from the last 24 hours and is event driven.

# Monitoring Interferers

In the Monitor > Wireless Technologies > Interferers page, you can monitor interference devices detected by CleanAir-enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

Table 19-1 lists the menu paths to follow to monitor interferers.

<table>
<thead>
<tr>
<th>To See...</th>
<th>Go To...</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP-detected interferers</td>
<td>Monitor &gt; Wireless Technologies &gt; Interferers</td>
</tr>
<tr>
<td>AP-detected interferer details</td>
<td>Monitor &gt; Wireless Technologies &gt; Interferers &gt; Interferer ID</td>
</tr>
<tr>
<td>AP-detected interferer details location history</td>
<td>Monitor &gt; Wireless Technologies &gt; Interferers &gt; Interferer ID, then choose Select a command &gt; Location History and click Go</td>
</tr>
</tbody>
</table>

Related topics
- Field Reference for AP-detected interferers
- Field Reference for AP-detected interferer details
- Field Reference for AP-detected interferer details location history

## Configuring the Search Results Display

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. To edit the columns in the AP Detected Interferers page, follow these steps:

**Step 1** Choose Monitor > Wireless Technologies > Interferers. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.

**Step 2** Click the Edit View link.

**Step 3** To add an additional column to the access points table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table.

**Step 4** To remove a column from the access points table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.

**Step 5** Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.
Step 6 Click **Reset** to restore the default view.

Step 7 Click **Submit** to confirm the changes.

## Monitoring RFID Tags

The **Monitor > Wireless Technologies > RFID Tags** page allows you to monitor tag status and location on Prime Infrastructure maps as well as review tag details.

This page is only available in the Location version of Prime Infrastructure.

This section provides information on the tags detected by the location appliance.

The Tag Summary page is available at **Monitor > Wireless Technologies > RFID Tags**.

### Searching RFID Tags

Use the Prime Infrastructure Advanced Search feature to find specific tags or all tags. To search for tags:

**Step 1** Click **Advanced Search**.

**Step 2** From the Search Category drop-down list, choose **Tags**.

**Step 3** Enter the required information. Note that search fields sometimes change, depending on the category chosen.

**Step 4** Click **Go**.

### Checking RFID Tag Search Results

To check the search results, click the MAC address of a tag location on a search results page.

Note the following:

- The Tag Vendor option does not appear when Asset Name, Asset Category, Asset Group, or MAC Address is the search criterion.
- Only vendor tags that support telemetry appear.
- The Telemetry data option appears only when MSE (select for location servers), Floor Area, or Outdoor Area is selected as the “Search for tags by” option.
- Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.
- Asset Information, Statistics, Location, and Location Notification details are displayed.
- Only CCX v1 compliant tags are displayed for emergency data.
Viewing Tag List

Click the **Total Tags number** link to view the Tags List for the applicable device name. The Tag List contains the MAC address, asset details, vendor name, mobility services engine, controller, battery status, and map location.

Monitoring Media Streams

To monitor the media streams configurations, follow these steps:

**Step 1** Choose **Monitor > Wireless Technologies > Media Streams**. The Media Streams page appears showing the list of media streams configured across controllers.

The Media Streams page contains a table with the following columns:

- **Stream Name**—Media Stream name.
- **Start IP**—Starting IP address of the media stream for which the multicast direct feature is enabled.
- **End IP**—Ending IP address of the media stream for which the multicast direct feature is enabled.
- **State**—Operational state of the media stream.
- **Max Bandwidth**—Indicates the maximum bandwidth that is assigned to the media stream.
- **Priority**—Indicates the priority bit set in the media stream. The priority can be any number from 1 to 8. A lower value indicates a higher priority. For example, a priority of 1 is highest and a value of 8 is the lowest.
- **Violation**—Indicates the action to performed in case of a violation. The possible values are as follows:
  - **Drop**—Indicates that a stream is dropped on periodic revaluation.
  - **Best Effort**—Indicates that a stream is demoted to best-effort class on periodic reevaluations.
- **Policy**—Indicates the media stream policy. The possible values are Admit or Deny.
- **Controllers**—Indicates the number of controllers that use the specified media stream.
- **Clients**—Indicates the number of clients that use the specified media stream.

**Step 2** To view the media stream details, click a media stream name in the Stream column. The Media Streams page appears.

The Media Streams page displays the following group boxes:

- **Media Stream Details**—Displays the media stream configuration information. This includes the Name, Start Address, End Address, Maximum Bandwidth, Operational Status, Average Packet Size, RRC Updates, Priority, and Violation.
- **Statistics**—Displays the number of controllers and number of clients that use the selected media stream. Click the controller count to access the list of controllers that use the selected media stream.
- **Error**—Displays the error, Worst AP, and corresponding floor map for that AP.
- **Client Counts**—Displays the number of clients for each period.
- **Failed Client Counts**—Displays the number of clients that failed for each period.
The client information is presented in a time-based graph. For graphs that are time-based, there is a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed.

Troubleshooting Unjoined Access Points

When a lightweight access point initially starts up, it attempts to discover and join a wireless LAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all the configuration details for the device and network. After successfully joining the wireless controller, the access point can be discovered and managed by Prime Infrastructure. Until the access point successfully joins a wireless controller the access point cannot be managed by Prime Infrastructure and does not contain the proper configuration settings to allow client access.

Prime Infrastructure provides you with a tool that diagnoses why an access point cannot join a controller and lists corrective actions.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included in the page. This includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason if known.

To troubleshoot unjoined access points, do the following:

**Step 1** Choose **Monitor > Wireless Technologies > Unjoined Access Points**. The Unjoined APs page appears containing a list of access points that have not been able to join a wireless controller.

**Step 2** Select the access point that you wish to diagnose, then click **Troubleshoot**. An analysis is run on the access point to determine the reason why the access point was not able to join a wireless controller. After performing the analysis, the Unjoined APs page displays the results.

**Step 3** If the access point has tried to join multiple wireless controllers and has been unsuccessful, the controllers are listed in the left pane. Select a controller.

**Step 4** In the middle pane, you can view what the problem is. It will also list error messages and controller log information.

**Step 5** In the right pane, recommendations for solving the problems are listed. Perform the recommended action.

**Step 6** If you need to further diagnose a problem, you can run RTTS through the Unjoined AP page. This allows you to see the debug messages from all the wireless controllers that the access point tried to join at one time.

To run RTTS, click the RTTS icon ( ) located to the right of the table. The debug messages appear in the table. You can then examine the messages to see if you can determine a cause for the access point not being able to join the controllers.
Monitoring Chokepoints

Chokepoints are low-frequency transmitting devices. When a tag passes within range of a placed chokepoint, the low-frequency field awakens the tag, which, in turn, sends a message over the Cisco Unified Wireless Network that includes the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room-level accuracy (ranging from few inches to 2 feet, depending on the vendor).

Chokepoints are installed and configured as recommended by the chokepoint vendor. After the chokepoint is installed and operational, it can be entered into the location database and plotted on a Prime Infrastructure map.

Related Topic
- Field Reference for Chokepoints Page

Adding a Chokepoint to the Prime Infrastructure Database

To add a chokepoint to the Prime Infrastructure database:

Step 1 Choose Monitor > Wireless Technologies > Chokepoints.
Step 2 From the Select a command drop-down list, choose Add Chokepoint.
Step 3 Click Go.
Step 4 Enter the MAC address and name for the chokepoint.
Step 5 Specify either an entry or exit chokepoint.
Step 6 Enter the coverage range for the chokepoint.
   Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.
Step 7 Click Save.
   After the chokepoint is added to the database, it can be placed on the appropriate Prime Infrastructure floor map.

Adding a Chokepoint to a Prime Infrastructure Map

To add a chokepoint to a map:

Step 1 Choose Maps > Wireless Maps > Site Maps.
Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.
Step 3 From the Select a command drop-down list, choose Add Chokepoints.
Step 4 Click Go.
   The Add Chokepoints summary page lists all recently added chokepoints that are in the database but not yet mapped.
Step 5 Select the check box next to the chokepoint that you want to place on the map.
Step 6 Click **OK**.

A map appears with a chokepoint icon located in the top-left corner. You are now ready to place the chokepoint on the map.

Step 7 Click the chokepoint icon and drag it to the proper location.

The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

Step 8 Click **Save**.

The newly created chokepoint icon might or might not appear on the map, depending on the display settings for that floor. The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you hover your mouse cursor over its map icon.

Step 9 If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Do not select the **Save Settings** check box unless you want to save this display criteria for all maps.

Step 10 Synchronize network design to the mobility services engine or location server to push chokepoint information.

---

### Removing a Chokepoint from the Prime Infrastructure Database

To remove a chokepoint from the Prime Infrastructure database:

1. Choose **Monitor > Wireless Technologies > Chokepoints**.
2. Select the check box of the chokepoint that you want to delete.
3. From the Select a command drop-down list, choose **Remove Chokepoints**.
4. Click **Go**.
5. Click **OK** to confirm the deletion.

---

### Removing a Chokepoint from a Prime Infrastructure Map

To remove a chokepoint from a Prime Infrastructure map:

1. Choose **Maps > Wireless Maps > Site Maps**.
2. In the Maps page, click the link that corresponds to the floor location of the chokepoint.
3. From the Select a command drop-down list, choose **Remove Chokepoints**.
4. Click **Go**.
Monitoring WiFi TDOA Receivers

The WiFi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset.

Enhancing Tag Location Reporting with WiFi TDOA Receivers

TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

**Note**

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network. See Adding MSEs to Prime Infrastructure.
2. Add the TDOA receiver to Prime Infrastructure database and map. See Adding WiFi TDOA Receivers to Prime Infrastructure and Maps.
3. Activate or start the partner engine service on the MSE using Prime Infrastructure.
4. Synchronize Prime Infrastructure and mobility services engines. See Synchronizing Prime Infrastructure and MSE.
5. Set up the TDOA receiver using the AeroScout System Manager. See the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User’s Guide for configuration details at the following URL:
Adding WiFi TDOA Receivers to Prime Infrastructure and Maps

After the WiFi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on a Prime Infrastructure map.

After adding TDOA receivers to Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than Prime Infrastructure.

For more details on configuration options, see the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide at the following URL:

To add a TDOA receiver to the Prime Infrastructure database and the appropriate map:

Step 1 Choose **Monitor > Wireless Technologies > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.
To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

Step 2 From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**.

Step 3 Click **Go**.

Step 4 Enter the MAC address, name, and static IP address of the TDOA receiver.

Step 5 Click **Save** to save the TDOA receiver entry to the database.

Note A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Step 6 Choose **Maps > Wireless Maps > Site Maps**.

Step 7 In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

Step 8 From the Select a command drop-down list, choose **Add WiFi TDOA receivers**.

Step 9 Click **Go**.

The All WiFi TDOA Receivers summary page lists all recently-added TDOA receivers that are in the database but not yet mapped.

Step 10 Select the check box next to each TDOA receiver to add it to the map.

Step 11 Click **OK**.

A map appears with a TDOA receiver icon located in the top-left corner. You are now ready to place the TDOA receiver on the map.

Step 12 Click the TDOA receiver icon and drag it to the proper location on the floor map.

Step 13 Click **Save**.

The icon for the newly added TDOA receiver might or might not appear on the map depending on the display settings for that floor. If the icon did not appear, proceed with Step 14.

Step 14 If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

Step 15 Select the **WiFi TDOA Receivers** check box.

When you hover your mouse cursor over a TDOA receiver on a map, configuration details appear for that receiver.
Step 16  Click X to close the Layers page.
Do not choose Save Settings from the Layers menu unless you want to save this display criteria for all maps.

Step 17  Download the partner engine software to the mobility services engine.
Using Monitoring Tools

- Monitoring Wireless Voice Audit
- Monitoring Wireless Voice Diagnostics
- Monitoring Wireless Configuration Audit
- Monitoring Autonomous AP Migration Analysis
- Monitoring Location Accuracy
- Monitoring Packet Capture

Monitoring Wireless Voice Audit

Prime Infrastructure provides a voice auditing mechanism to check controller configuration and to ensure that any deviation from the deployment guidelines is highlighted as an Audit Violation. You can run a voice audit on a maximum of 50 controllers in a single operation.

To run the voice audit:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Monitor &gt; Tools &gt; Wireless Voice Audit</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the <strong>Controllers</strong> tab, and complete the fields as described in the Voice Audit Field Descriptions section in the <em>Cisco Prime Infrastructure 3.1 Reference Guide</em>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the <strong>Rules</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the VoWLAN SSID text box, type the applicable VoWLAN SSID.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Do either of the following:</td>
</tr>
<tr>
<td></td>
<td>• To save the configuration without running a report, click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>• To save the configuration and run a report, click <strong>Save and Run</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click the <strong>Report</strong> tab to view the report results.</td>
</tr>
</tbody>
</table>
Monitoring Wireless Voice Diagnostics

The Voice Diagnostic tool is an interactive tool that diagnoses voice calls in real time. This tool reports call control errors, clients’ roaming history, and the total number of active calls accepted and rejected by an associated AP.

The Voice Diagnostic test is provisioned for multiple controllers; that is, if the AP is associated with more than one controller during roaming, the Voice Diagnostic tool tests all associated controllers. Prime Infrastructure supports testing on controllers whose APs are placed on up to three floors. For example, a Prime Infrastructure map might have floors 1 to 4, with all APs associated to controllers (WLC1, WLC2, WLC3, and WLC4) and placed on the Prime Infrastructure map. If a client on any AP is associated with WLC1 on the first floor and a Voice Diagnostic test is started for that client, a test is also provisioned on WLC2 and WLC3.

The Voice Diagnostic page lists prior test runs, if any. For information about the fields on this page, see the Voice Diagnostic Field Descriptions section in the Cisco Prime Infrastructure 3.1 Reference Guide.

From the Select a command from the drop-down list, you can start a new test, check the results of an existing test, or delete a test.

**Note**

To support roaming, the tool figures out controllers in the same building as of client’s associated AP building and adds to all controller’s watchlist. The tool looks for controllers in +/-5 floors from client’s current association A’s location to configure on controllers. Configuration on controller’s watchlist is done for 10 minutes. After 10 minutes controller will remove the entry from the watchlist.

To run a Voice Diagnostic test:

**Step 1** Choose Monitor > Tools > Wireless Voice Diagnostic.

**Step 2** From the Select a command drop-down list, choose the New test and click Go.

**Note** You can configure a maximum of two clients for voice call diagnosis. Both clients can be on the same call or can be on a different call.

**Step 3** Enter a test name and the length of time to monitor the voice call.

**Step 4** Enter the MAC address of the device for which you want to run the voice diagnostic test.

**Step 5** Select a device type; if you select a custom phone, enter an RSSI range.

**Step 6** Click StartTest.

Monitoring Wireless Configuration Audit

Choose Monitor > Tools > Wireless Configuration Audit to launch the Configuration Audit Summary page.

This page provides a summary of the following:

- Total Enforced Config Groups—Templates that are configured for Background Audit and are enforcement enabled.
• Total Mismatched Controllers—Configuration differences found between Prime Infrastructure and the controller during the last audit.

• Total Config Audit Alarms—Alarms generated when audit discrepancies are enforced on configuration groups. If enforcement fails, a critical alarm is generated on the configuration group. If enforcement succeeds, a minor alarm is generated on the configuration group. Alarms contain links to the audit report, where you can view a list of discrepancies for each controller.

• Most recent 5 config audit alarms—Includes object name, event type, date, and time of the audit alarm.

Click View All to view the applicable Alarm page that includes all configuration audit alarms.

Monitoring Autonomous AP Migration Analysis

Choose Monitor > Tools > Autonomous AP Migration Analysis to launch the Migration Analysis Summary page.

Autonomous access points are eligible for migration only if all criteria have a pass status. A red X designates ineligibility, and a green check mark designates eligibility. These columns represent the following:

• Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.

• Software Version—Conversion is supported only from Cisco IOS 12.3(7)JA releases excluding Cisco IOS 12.3(11)JA, Cisco IOS 12.3(11)JA1, Cisco IOS 12.3(11)JA2, and Cisco IOS 12.3(11)JA3.

• Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  – root
  – root access point
  – root fallback repeater
  – root fallback shutdown
  – root access point only

• Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

Monitoring Location Accuracy

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy tool.

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

The Location Accuracy tool enables you to run either of the following tests:
Monitoring Location Accuracy

- **Scheduled Accuracy Testing**—Employed when clients, tags, and interferers are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients, tags, and interferers are already prepositioned so that the test can be run on a regularly scheduled basis.

- **On-Demand Accuracy Testing**—Employed when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

Both are configured and executed through a single page.

**Enabling the Location Accuracy Tool**

You must enable the **Advanced Debug** option in Prime Infrastructure to use the Scheduled and On-demand location accuracy tool testing features. The Location Accuracy tool does not appear as an option on the Monitor > Tools menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in Prime Infrastructure:

1. In Prime Infrastructure, choose Maps > Wireless Maps > Site Maps.
2. Choose Properties from the Select a command drop-down list, and click Go.
3. Select the **Enabled** check box to enable the Advanced Debug Mode. Click OK.

**Note**

If Advanced Debug is already enabled, you do not need to do anything further. Click **Cancel**.

Use the Select a command drop-down list in the Location Accuracy page, to create a new scheduled or on-demand accuracy test, to download logs for last run, to download all logs, or to delete a current accuracy test.

**Note**

- You can download logs for accuracy tests from the Accuracy Tests summary page. To do so, select an accuracy test and from the Select a command drop-down list, choose either **Download Logs** or **Download Logs for Last Run**. Click **Go**.
- The Download Logs option downloads the logs for all accuracy tests for the selected test(s).
- The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

**Scheduling a Location Accuracy Test**

Use the scheduled accuracy testing to verify the accuracy of the current location of non-rogue and rogue clients, interferers, and asset tags. You can get a PDF of the test results at **Accuracy Tests > Results**. The Scheduled Location Accuracy report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
### Monitoring Location Accuracy

- An error distance histogram.
- A cumulative error distribution graph.
- An error distance over time graph.
- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location), and error distance over time for each MAC.

To schedule a Location Accuracy test:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Monitor &gt; Tools &gt; Location Accuracy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose New Scheduled Accuracy Test from the Select a command drop-down list.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter a test name.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Choose an area type, a building, and a floor from the corresponding drop-down lists.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Campus is configured as Root Area, by default. There is no need to change this setting.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose a beginning and ending time for the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When entering the test start time, be sure to allow enough time prior to the test start to position testpoints on the map.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose Administration &gt; Settings &gt; System Settings &gt; Mail Server Configuration to enter the appropriate information.)</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click Position Test Points.</td>
</tr>
<tr>
<td>Step 8</td>
<td>On the floor map, select the check box next to each client, tag, and interferer for which you want to check location accuracy.</td>
</tr>
<tr>
<td></td>
<td>When you select a MAC address check box, two icons appear on the map. One represents the actual location and the other represents the reported location. If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map. (You cannot drag the reported location.)</td>
</tr>
<tr>
<td>Step 9</td>
<td>(Optional) To enter a MAC address for a client, tag, or interferer that is not listed, select the Add New MAC check box, enter the MAC address, and click Go.</td>
</tr>
<tr>
<td></td>
<td>An icon for the newly added element appears on the map. If the element is on the location server but on a different floor, the icon appears in the left-most corner (in the 0,0 position).</td>
</tr>
<tr>
<td>Step 10</td>
<td>When all elements are positioned, click Save.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Click OK to close the confirmation dialog box.</td>
</tr>
<tr>
<td></td>
<td>You are returned to the Accuracy Tests summary page.</td>
</tr>
<tr>
<td>Step 12</td>
<td>To check the test results, click the test name, click the Results tab in the page that appears, and click Download under Saved Report.</td>
</tr>
</tbody>
</table>
Running an On-Demand Location Accuracy Test

You can run an On-Demand Accuracy Test when elements are associated but not prepositioned. On-Demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy of a small number of clients, tags, and interferers. You can get a PDF of the test results at Accuracy Tests > Results. The On-Demand Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram
- A cumulative error distribution graph

To run an On-Demand Accuracy Test:

Step 1 Choose Monitor > Tools > Location Accuracy.
Step 2 From the Select a command drop-down list, choose New On demand Accuracy Test.
Step 3 Enter a test name.
Step 4 Choose an area type, a building, and a floor from the corresponding drop-down lists.

**Note** Campus is configured as Root Area, by default. There is no need to change this setting.

Step 5 Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose Administration > Settings > System Settings > Mail Server Configuration to enter the appropriate information.)
Step 6 Click Position Test Points.
Step 7 To test the location accuracy and RSSI of a particular location, select client, tag, or interferer from the drop-down list on the left. A list of all MAC addresses for the selected option (client, tag, or interferer) is displayed in a drop-down list to the right.
Step 8 Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.
Step 9 From the Zoom percentage drop-down list, choose the zoom percentage for the map.
The X and Y text boxes are populated with the coordinates based on the position of the red cross hair in the map.
Step 10 Click Start to begin collection of accuracy data, and click Stop to finish collection. You must allow the test to run for at least two minutes before stopping the test.
Step 11 Repeat Step 7 to Step 10 for each testpoint that you want to plot on the map.
Step 12 Click Analyze Results when you are finished mapping the testpoints, and then click the Results tab in the page that appears to view the report.
Monitoring Packet Capture

In addition to aggregating data from multiple NAMs, Prime Infrastructure with licensed Assurance features makes it easy to actively manage and troubleshoot network problems using multiple NAMs and ASRs. For details, see Using Packet Capture to Monitor and Troubleshoot Network Traffic.
Viewing Performance Graphs

To compare the Key Performance Indicators (KPIs) for devices and interfaces, choose Monitor > Monitoring Tools > Performance Graphs. You can choose the device or interface metrics you want to view over a specified time, and the resulting performance graphs allow you to quickly monitor performance.

Creating Performance Graphs

**Step 1** Choose Monitor > Monitoring Tools > Performance Graphs.

The first time you access this page, an overlay help window appears with helpful tips.

**Step 2** Select one of the tabs at the top of the left frame:
- **Devices**—Allows you to select a device for which to create a performance graph.
- **Interfaces**—Allows you to select an interface for which to create a performance graph.

Depending on what you select, the Metrics panel displays the available metrics for the device or interface type.

**Step 3** Hover your cursor over a metric for which you want to measure performance, then click and drag the metric onto the Graphs portion of the window.

An overlay help window appears explaining the icons, date range, and other information.

Related Topics

- Viewing Multiple Metrics on a Single Performance Graph
- Performance Graphs Options

Viewing Multiple Metrics on a Single Performance Graph

You might want to view more than one metric on a single performance graph. For example, if you see a spike in CPU utilization, you might add the memory utilization metric to the performance graph to see if the memory was impacted by change in CPU utilization.

You can add a maximum of 10 metrics on a single performance graph.
Chapter 21      Viewing Performance Graphs

Performance Graphs Options

Step 1  Choose Monitor > Monitoring Tools > Performance Graphs.

Step 2  Select one of the tabs at the top of the left frame:

- **Devices**—Allows you to select a device for which to create a performance graph.
- **Interfaces**—Allows you to select an interface for which to create a performance graph.

Depending on what you select, the Metrics panel displays the available metrics for the device or interface type.

Step 3  Hover your cursor over a metric for which you want to measure performance, then click and drag the metric on to the Graphs portion of the window.

Step 4  To add a second metric to the same graph, hover your cursor over the metric you want to add, then click and drag the metric on to the same graph that has the metric you added in the previous step.

If you don’t want multiple metrics in a single graph, you can create a new graph on the same page by dragging the metric on to the lower portion of the Graphs window where Drop item here is displayed.

Step 5  To launch the Device 360° View, click on the IP address hyperlink at the top of the graph.

Related Topics

- Creating Performance Graphs
- Performance Graphs Options

Performance Graphs Options

The **Show** menu at the top of the performance chart allows you to change the following graph display options:

- **Legend Options**—Specify whether to show or hide the legend.
- **Show Legends**—Specify if the legends are at the right or the top of the performance chart.
- **Show Alarms**—Specify whether to display alarms. A colored flag appears in the performance graph to indicate that an alarm occurred at that time. To view details about the alarm, click on the colored flag.
- **Show Config Changes**—Specify whether to display configuration changes. A black flag appears in the performance graph to indicate that a configuration on the device was modified at that time. To view details about the configuration change, click on the flag.

You can also Export and Print performance graphs by clicking the arrow at the top of the graph.

Click **Detach** at the top right of the performance graph page to open the performance graph in a new browser window. This allows you to continue monitoring the performance graph in a separate window while you perform actions in another window.

You can draw up to 10 charts on each tab and up to 7 series in each chart. Any additional charts or series over these limits are not displayed and a warning message appears. To add additional charts, add a new tab and add additional charts you want to plot to the new tab.

If you plot a parent group with more than 7 items, the items are drawn in one chart to allow you to view the data for the entire group.
Related Topics

- Creating Performance Graphs
- Viewing Multiple Metrics on a Single Performance Graph
Troubleshooting

Cisco Prime Infrastructure provides the following for sophisticated monitoring and troubleshooting of end-user network access.

The following sections describe some typical troubleshooting tasks:

- Getting Help from Cisco
- Checking an End User’s Network Session Status
- Troubleshooting Authentication and Authorization
- Troubleshooting Network Attachments
- Troubleshooting Network Attachment Devices
- Troubleshooting Site Network Devices
- Troubleshooting the User Application and Site Bandwidth Utilization
- Troubleshooting User Problems
- Troubleshooting the User’s Experience
- Troubleshooting Voice/Video Delivery to a Branch Office
- Troubleshooting Unjoined Access Points
- Troubleshooting Wireless Performance Problems

Getting Help from Cisco

Prime Infrastructure provides helpful tools for network operators to connect to Cisco experts to diagnose and resolve problems. You can open support cases and track your cases from Prime Infrastructure. If you need help troubleshooting any problems, Prime Infrastructure allows you to:

- Connect with the Cisco Support Community to view and participate in discussion forums. See Launching the Cisco Support Community.
- Open a support case with Cisco Technical Support. See Opening a Support Case.

Launching the Cisco Support Community

You can use Prime Infrastructure to access and participate in discussion forums in the online Cisco Support Community. This forum can help you find information for diagnosing and resolving problems.

You must enter your Cisco.com username and password to access and participate in the forums.
Checking an End User’s Network Session Status

When an end user calls the help desk, typically with a complaint that might not be very specific (“I can’t log in” or “The network is really slow”), you will want to get an overall view of the user’s current network session status, identify which individual session is associated with the problem, and examine the details for that session.

To launch the Cisco Support Community:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Monitor &gt; Monitoring Tools &gt; Alarms &amp; Events, select an alarm, then choose Troubleshoot &gt; Support Forum.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Cisco Support Community Forum page, enter additional search parameters to refine the discussions that are displayed.</td>
</tr>
</tbody>
</table>

Opening a Support Case

You can use Prime Infrastructure to open a support request and to track your support cases. Prime Infrastructure helps you gather critical contextual information to be attached to the support case, reducing the time it takes to create a support case.

To open a support case or access the Cisco Support Community, you must:

- Have a direct Internet connection on the Prime Infrastructure server
- Enter your Cisco.com username and password

To open a support case:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Chose Monitor &gt; Monitoring Tools &gt; Alarms &amp; Events, then hover your mouse cursor over the IP address of the device on which the alarm occurred.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the device 360° view, Select Support Request from Actions drop-down menu.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter your Cisco.com username and password.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Login.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Create in Update or Create a Support Case window.</td>
</tr>
<tr>
<td></td>
<td>Prime Infrastructure gathers information about the device and populates the fields for which it can retrieve information. You can enter a Tracking Number that corresponds to your own organization’s trouble ticket system.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Next and enter a description of the problem.</td>
</tr>
<tr>
<td></td>
<td>By default, Prime Infrastructure enters information that it can retrieve from the device. Prime Infrastructure automatically generates the necessary supporting documents such as the technical information for the device, configuration changes, and all device events over the last 24 hours. You can also upload files from your local machine.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click Create Service Request.</td>
</tr>
</tbody>
</table>
For example, how is the user attached to the network? Does this person have more than one endpoint (where an endpoint could be, for example, a laptop, desktop, iPad, iPhone, or Android)?

Before You Begin
This feature requires:
- Integration with an ISE server (to access endpoint information).
- Integration with LDAP (to display information about the end user).

To check an end user’s network session status:

Step 1 In the system search field (see Search Methods), enter the name of the user (or client) who is experiencing the issue. If there are multiple matches, select the correct username from the list of matches.

Step 2 Start the User 360° View.

The information that is available from this view typically includes current information about the end user and all of that user’s current or recently ended network sessions.

Troubleshooting Authentication and Authorization

Using the User 360° View, you can identify possible problems with the end user’s authentication and authorization for network access.

For example, there could be authentication problems (such as the user’s password being rejected), or there could be authorization issues (such as the user being placed in a policy category such as “guest” or “quarantine” that might result in unexpected behavior).

Before You Begin
This feature requires integration with an ISE server.

To troubleshoot the network:

Step 1 Open the User 360° View for that user and check the value in “Authorization Profile”. This is a mnemonic string that is customer-defined, so it might not contain clear information (for example, “standard_employee” or “standard_BYOD” or “Guest”).

Step 2 If this field is a link, click it to display information about the user’s authorization profile. Based on this information:
- If the end user is associated with the appropriate policy category, this procedure is complete.
- If the end user is not associated with the appropriate policy category, you can hand off the problem (for example, to an ISE admin or help tech) or perform actions outside Prime Infrastructure to investigate why the user was placed in the current policy category (Authorization Profile).

Step 3 Check to see whether there are any indications of authentication errors (authentication failure could be due to various things, including an expired password). The visual indication of authentication errors allows you to see more data related to the authentication errors. At that point, you might need to hand off the problem (for example, to an ISE admin or help tech).
Troubleshooting Network Attachments

Use the following procedure to determine if there are problems with the end user attaching to the network, such as errors on the access port (wired) or radio association problems (wireless).

To troubleshoot network attachments:

**Step 1** Open the User 360° View for that user and click the Go to Client Details icon.

**Step 2** If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note the problem and hand it off to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose Monitor > Monitoring Tools > Clients and Users).

Troubleshooting Network Attachment Devices

Use the following procedure to troubleshoot any active alarms or error conditions associated with the network attachment device and port for the end user that might be causing problems for the end user’s network session:

**Step 1** To view any existing active alarms or error conditions associated with the network attachment device and port for the end user (available for the controller, switch, access point, and site), open the User 360° View for that user and click the Alarms tab.

**Step 2** To see if a problem has been detected, click the Go to Client Details icon.

**Step 3** If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note that fact and hand off the task to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose Monitor > Monitoring Tools > Clients and Users).

Troubleshooting Site Network Devices

Use the following procedure to determine if there are any existing active alarms or error conditions associated with any of the network devices that are part of the site for the end user that could be causing problems for the user’s network session.

**Step 1** To view any existing active alarms or error conditions associated with network devices that are part of the site for the end user, open the User 360° View for that user and click the Alarms tab.

**Step 2** You can choose to view:
- Active alarms list for the site
- List of all site devices (with alarm indications)
- Topo map of site (with alarm indications)
Step 3 If a problem with a site has been detected, an alarm icon will appear next to the site location. Click the icon to view all of the alarms associated with that site.

Step 4 If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note that fact and hand off the task to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose Monitor > Monitoring Tools > Clients and Users).

Troubleshooting the User Application and Site Bandwidth Utilization

If an end user is experiencing high bandwidth utilization for a site on the interface dashboard, use the following procedure to identify the applications consumed by the user and the bandwidth consumed by every application for a given endpoint owned by the user.

Before You Begin
This feature requires:
• Integration with an ISE server (to access endpoint information).
• For wired sessions, that AAA accounting information is being sent to ISE.
• That session information (netflow/NAM data, Assurance licenses) is available.

Step 1 To view the applications accessed by the end user and the response time for the applications for the user’s devices, open the User 360° View for that user and click the Applications tab.

Step 2 The Applications tab displays information about the applications accessed by the end user (see Troubleshooting). To get more information about an application, including the bandwidth utilization of the application consumed by the end user (the bandwidth consumed for the conversation), choose Dashboard > Performance > Application.
Troubleshooting User Problems

You can use the User 360° View to troubleshoot problems reported by users.

---

**Step 1**  In the Search field on any page, enter the end user’s name.

**Step 2**  In the Search Results window, hover your mouse cursor over the end user’s name in the User Name column, then click the User 360° view icon that appears as shown in Figure 60-6.

**Step 3**  With the User 360° view displayed, identify where the problem is occurring using the information described in Table 22-1.

---

Table 22-1  Using the User 360° View to Diagnose User Problems

<table>
<thead>
<tr>
<th>To Gather This Data</th>
<th>Click Here in User 360° View</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information about the device to which the user is attached, such as the endpoint, location, connections, and session information</td>
<td>Click a device icon at the top of the User 360° View.</td>
<td>Click available links to display additional information. For example, you can click the Authorization Profile link to launch ISE. See Troubleshooting Authentication and Authorization</td>
</tr>
<tr>
<td>Alarms associated with the device to which the user is attached</td>
<td>Click a device icon at the top of the User 360° View, then click the <strong>Alarms</strong> tab.</td>
<td>Click the Troubleshoot Client icon to go to client troubleshooting.</td>
</tr>
<tr>
<td>Applications running on the device to which the user is attached</td>
<td>Click a device icon at the top of the User 360° View, then click the <strong>Applications</strong> tab.</td>
<td>Click an application to view the end-user data filtered for the user you specified. See Troubleshooting the User’s Experience.</td>
</tr>
</tbody>
</table>

---

Troubleshooting the User’s Experience

If an end user reports a problem with accessing the application, use the User 360° View to troubleshoot the user’s experience.

**Before You Begin**

This feature requires that session information (netflow/NAM data, Assurance licenses) is available.

---

**Step 1**  To view the applications accessed by the end user and the response time for the applications for the user’s devices, open the User 360° View for that user and click the **Applications** tab.

**Step 2**  The Applications tab displays information about the applications accessed by the end user (see Troubleshooting User Problems). To get more information about an application, choose **Dashboard > Performance > Application**.
Troubleshooting Voice/Video Delivery to a Branch Office

To successfully diagnose and resolve problems with application service delivery, network operators must be able to link user experiences of network services with the underlying hardware devices, interfaces, and device configurations that deliver these services. This is especially challenging with RTP-based services like voice and video, where service quality, rather than gross problems like outages, impose special requirements.

Note

To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

Prime Infrastructure with the licensed Assurance features makes this kind of troubleshooting easy. The following workflow is based on a typical scenario: The user complains to the network operations desk about poor voice quality or choppy video replay at the user’s branch office. The operator first confirms that the user is indeed having a problem with jitter and packet loss that will affect the user’s RTP application performance. The user further confirms that other users at the same branch are also having the same problem. The operator next confirms that there is congestion on the WAN interface on the edge router that connects the local branch to the central voice/video server in the main office. Further investigation reveals that an unknown HTTP application is using a high percentage of the WAN interface bandwidth and causing the dropouts. The operator can then change the unknown application’s DSCP classification to prevent it from stealing bandwidth.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Dashboard &gt; Performance &gt; End User Experience.</td>
</tr>
</tbody>
</table>
| Step 2 | Next to Filters, specify:  
  - The IP address of the Client machine of the user complaining about poor service.  
  - The Time Frame during which the problem occurred.  
  - The ID of the problem Application. |
| Step 3 | View Average Packet Loss to see the Jitter and Packet Loss statistics for the client experiencing the problem. |
| Step 4 | View the User Site Summary to confirm that other users at the same site are experiencing the same issue with the same application. |
| Step 5 | In the User Site Summary, under Device Reachability, hover your mouse cursor over the branch’s edge router. Prime Assurance displays a 360° View icon for the device under the Device IP column. Click the icon to display the 360° View. |
| Step 6 | In the 360° View, click the Alarms tab, to see alarms on the WAN interfaces, or on the Interfaces tab, to see congested WAN interfaces and the top applications running on them. |

Troubleshooting Unjoined Access Points

When a lightweight access point initially starts up, it attempts to discover and join a wireless LAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all of the configuration details for the device and network. Until the access point
Troubleshooting Unjoined Access Points

If an access point successfully joins a wireless controller, it cannot be managed by Prime Infrastructure, and it does not contain the proper configuration settings to allow client access. Prime Infrastructure provides you with a tool that diagnoses why an access point cannot join a controller, and lists corrective actions.

Note
To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included on the page. This information includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason, if known.

To troubleshoot unjoined access points:

Step 1 Choose Monitor > Wireless Technologies > Unjoined Access Points.
Step 2 In the Unjoined APs page, select an access point to diagnose, then click Troubleshoot.
Step 3 After the troubleshooting analysis runs, check the results in the Unjoined APs page.
Step 4 Select a controller and check the middle pane for:
   - A statement of the problem
   - A list of error messages
   - Controller log information
Step 5 Check the right pane for recommendations for solving any problems, and perform any recommended actions.
Step 6 (Optional) To further diagnose the problem, run RTTS through the Unjoined AP page by clicking the RTTS icon located to the right of the table. Examine the debug messages that appear in the table to determine a cause for the access point being unable to join the controllers.

RTTS Debug commands for Troubleshooting Unjoined Access Points

Table 22-2 contains the list of RTTS debug commands for Legacy controllers and NGWC controllers.

<table>
<thead>
<tr>
<th>Controller</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy</td>
<td>• debug capwap info enable</td>
</tr>
<tr>
<td></td>
<td>• debug dot1x all enable</td>
</tr>
<tr>
<td></td>
<td>• debug mobility directory enable</td>
</tr>
<tr>
<td>NGWC</td>
<td>• debug capwap ap error</td>
</tr>
<tr>
<td></td>
<td>• debug dot1x events</td>
</tr>
<tr>
<td></td>
<td>• debug capwap ios detail</td>
</tr>
</tbody>
</table>
Troubleshooting Wireless Performance Problems

If an end user reports a problem with their wireless device, you can use the Site dashboard to help you determine the AP that is experiencing problems.

**Before You Begin**
This feature requires that session information (netflow/NAM data, Assurance licenses) is available.

**Step 1**
Choose Dashboard > Performance > Site and view the site to which the client experiencing trouble belongs.

**Step 2**
To see the AP that is experiencing trouble at this site, click the Settings icon, then click Add next to Busiest Access Points.

**Step 3**
Scroll down to the Busiest Access Points dashlet. You can
- Hover your mouse over a device to view device information. See Getting Device Details from Device 360° View.
- Click on an AP name to go to the AP dashboard from where you can use the AP filter option to view AP details such as Client Count, Channel Utilization, and, if you have an Assurance license, Top N Clients and Top N Applications.
- Utilization based on SNMP polling for the APs.
- Volume information based on Assurance NetFlow data, if you have an Assurance license. For example, you can see the traffic volume per AP.

Root Cause and Impact analysis of Physical and Virtual Data Center Components

The physical servers shows the list of UCS B-Series and C-series servers that are managed by Prime Infrastructure. It also shows the Host/Hypervisor running on these servers, only if the corresponding Vcenter is added.

The Cisco UCS Server Schematic shows the complete architecture of the UCS device. The Schematic tab shows a graph that can be expanded to show different elements of UCS device such as chassis and blades. You can view quick summary of the element by hovering your mouse over the operational status icon next to the chassis or blade. In addition, clicking on the operational status icon, which symbolizes each unique element (chassis or blade), would show the subsequent connection. You can view the connection to host and its VM if managed by Prime Infrastructure by clicking the operational status icon. The schematic view also shows the operational status of the data center components and the associated alarms using which you can trace the root cause of an application delivery failure to a UCS hardware problem of Cisco UCS device.

Troubleshooting UCS Hardware Problems

Use the following procedure to trace the root cause of an application delivery failure to a UCS hardware problem of Cisco UCS B-series and C-series servers. You can identify whether the problem is in fabric interconnect port, chassis or blades.
To identify the issue in UCS chassis, blade server, fabric interconnect port:

**Step 1** Choose **Inventory > Device Management > Compute Devices.**

**Step 2** Choose **Cisco UCS Servers** in the **Compute Devices** pane.

**Step 3** Click the faulty UCS device in the **Cisco UCS Servers** pane to view the **Schematic** tab that shows the inter-connections of the UCS chassis and blades, and the up/down status of chassis and blade servers. Hover your mouse over the faulty chassis or blade server name to view the Quick Summary of the element.

If you want to view the detailed information about the faulty chassis or blade server, click **View 360.**

**Step 4** Click the **Chassis** tab and hover your mouse cursor over the faulty chassis name, then click the information icon to launch the chassis 360° view that shows up/down status of power supply unit and fan modules.

**Step 5** Click the **Servers** tab and hover your mouse cursor over the faulty blade server name, then click the information icon to launch the server 360° view.

The server 360° view provides detailed blade server information including the number of processors, memory capacity, up/down status of adapters, Network Interface Cards (NICs), and Host Bus Adapters (HBAs) and Service Profile.

**Step 6** Click the **Network** tab to view the entire network interface details of fabric interconnect such as port channel, Ethernet interface, vEthernet, and vFabric Channel.

**Step 7** Click the **IO Modules** tab to view the operational status of backplane ports and fabric ports.

**Step 8** Click the **Service Profile** tab to view the hardware faults that impacts the services.

**Step 9** In the **Service Profile** pane on the left, click the expand icon to view the service profiles.

**Step 10** Click the information icon corresponding to the service profile to view the alarm severity levels of that service profile.

**Step 11** Click the faulty service profile in the **Service Profile** pane on the left to view the **Service Profile** table that displays the Profile Name, Service Profile Template, Server, Overall Status, Associated status and Associated Alarms.

**Step 12** Click the information icon corresponding to the profile name in the **Service Profile** table to launch the Service Profile 360° view that shows the basic summary information of the service profile.

To identify the bandwidth issue in fabric interconnect port:

**Step 1** Choose **Inventory > Device Management > Network Devices.**

**Step 2** Click the faulty UCS device from the **All Devices** pane.

**Step 3** Click the expand icon corresponding to fabric interconnect switch.

**Step 4** Click **Fixed Modules** to view the operational status of fabric interconnect ports.

**Step 5** Click **Interfaces** to view the operational status for fabric interconnect port and interfaces. This is same as the operational stays of fabric interconnect port and interfaces viewed from **Network** tab in Compute Devices page.
Viewing Bandwidth on Fabric Interconnect Ports

You can view the details of a fabric interconnect port or a fabric interconnect port group using the Top-N Interface Utilization dashlet from the Overview and Performance dashboards. Use the following procedure to identify whether the overuse of bandwidth on the ports connecting the fabric interconnect to the UCS chassis is causing application performance issues such as slowness on Cisco UCS.

We recommend you to create a fabric interconnect port group and select the port group in the dashlet to view the bandwidth utilization details.

To identify the overuse of bandwidth on the fabric interconnect ports:

---

**Step 1** Choose Dashboard > Performance > Interface then choose the UCS device interface from the Interface drop-down list.

or

Choose Dashboard > Overview > Network Interface.

**Step 2** Click the Settings icon as shown in and choose Add Dashlets.

**Step 3** Choose Top N Interface Utilization dashlet and click Add.

**Step 4** Do the following if you have already created a fabric interconnect port group

a. Click the Dashlet Options icon in the Top N Interface Utilization dashlet.

b. Select the fabric interconnect port group in the Port Group and click Save And Close.

The Top N Interface Utilization dashlet displays the list of interfaces with maximum utilization percentage. This dashlet also shows the average and maximum data transmission and reception details of the fabric interconnect ports.
Monitoring Multiple Prime Infrastructure Instances

There are three situations in which you will want to use multiple Cisco Prime Infrastructure server instances to manage your network:

- You want to categorize the devices in your network into logical groups, with a different Prime Infrastructure instance managing each of those groups. For example, you could have one instance managing all of your network’s wired devices and another managing all of its wireless devices.
- The one Prime Infrastructure instance you have running is sufficient to manage your network, but the addition of one or more instances would improve Prime Infrastructure’s performance by spreading the CPU and memory load among multiple instances.
- Your network has sites located throughout the world, and you want a different Prime Infrastructure instance to manage each of those sites in order to keep their data separate.

If multiple Prime Infrastructure instances are running in your network, you can monitor those instances from the Operations Center. In this chapter, we will cover a typical workflow you might employ when using the Operations Center. This workflow consists of the following tasks:

- Viewing the Operations Center dashboards
- Configuring devices using Prime Infrastructure templates
- Monitoring your network
- Running reports

See Related Topics for details on these and related tasks.

Related Topics

- Setting Up Operations Center
- Viewing the Operations Center Dashboards
- Configuring Devices Using Operations Center
- Monitoring Your Network Using Operations Center
- Running Reports With Operations Center
- Operations Center FAQs
Viewing the Operations Center Dashboards

The Operations Center provides additional, Operations Center-specific dashboards that you can use to quickly determine the status of your network and identify any issues that require further attention. The Operations Center dashlets display aggregated data. The following types of dashboards are available:

- Overview dashboards, which summarize the current status of key areas in your network.
- Incident dashboards, which report on all alarms and events recorded across your network.

To access a particular dashboard and the dashlets that comprise it, either click the appropriate tabs on the main Operations Center page or select the dashboard from the Dashboard menu.

For general information about using and customizing dashboards and dashlets, see “Prime Infrastructure User Interface Reference” in Related Topics.

Related Topics
- Setting Up Operations Center
- Monitoring Your Network Using Operations Center
- Appendix 60, “Prime Infrastructure User Interface Reference.”
- Operations Center FAQs

Configuring Devices Using Operations Center

Although it does not directly manage or configure any device in your network, Operations Center gives you access to the configuration templates stored on the Prime Infrastructure server instances it manages. You can use Operations Center to:

- View the configuration templates on any of the Prime Infrastructure servers,
- Distribute templates that exist on one server to any of the other servers Operations Center manages. Template distribution like this is required if (for example) you want to deploy a template across your entire network.

The steps for doing these tasks are identical to the ones you follow when you perform the same tasks on standalone Prime Infrastructure servers. You simply need to log into the Operations Center instance first, and then select the Prime Infrastructure server instance whose templates you want to work on.

See the following Related Topics for more details.

Related Topics
- Viewing Configuration Templates Using Operations Center
- Distributing Configuration Templates Across Managed Servers
- Monitoring Your Network Using Operations Center

Viewing Configuration Templates Using Operations Center

You can view configuration templates on any managed Prime Infrastructure instance by selecting the Configuration menu option in Operations Center and expanding the listing until you find the templates you want.
Chapter 23      Monitoring Multiple Prime Infrastructure Instances

Configuring Devices Using Operations Center

Step 1
Log in to Operations Center and choose Configuration > Templates > Features & Technologies.

Step 2
Expand the template category you want to view (for example, My Templates). Operations Center display a list of the managed Prime Infrastructure instances with templates in that category.

Step 3
Expand the managed instance whose templates you want to view. Expand the template sub-categories as needed.

Related Topics
- Distributing Configuration Templates Across Managed Servers
- Configuring Devices Using Operations Center
- Creating Feature-Level Configuration Templates
- Deploying Templates

Deploying Configuration Templates

Step 1
After you create a configuration template, click Deploy. The Deployment wizard page opens.

Step 2
Select the devices on which you want to deploy the template, then click Next to choose the input values.

Step 3
In the Input Values tab, you can toggle between Form and CLI view.

Step 4
After entering the necessary configuration values, click Next or click CLI to confirm the device and template configuration values.

Step 5
Click Next to view the job deployment summary.

Step 6
On the Deployment Summary tab, you will see the CLI view for each of the device.

Step 7
Click Finish to deploy the template.

Distributing Configuration Templates Across Managed Servers

You can copy any user-defined configuration template on any managed Prime Infrastructure instance to another managed instance by selecting that template and clicking Distribute.

Distributing a template to another Prime Infrastructure server instance occurs automatically when you deploy a template to a device on another such instance without first copying (distributing) that template to the other instance.

Step 1
Log in to Operations Center and choose Configuration > Templates > Features & Technologies.

Step 2
Expand the template category you want to view (for example, My Templates). Operations Center displays a list of the managed Prime Infrastructure instances with templates in that category.

Step 3
Expand the managed instance whose templates you want to view. Expand the template sub-categories as needed.

Step 4
When you see the template you want to distribute, click on it to select it. Operations Center displays details for the selected template.
Step 5
Click Distribute. Operations Center displays a list of all the Prime Infrastructure server instances that it manages and that are currently reachable.

Step 6
Select the checkbox next to each Prime Infrastructure server instance to which you want to distribute the template, then click OK.
If the template already exists on the other server, Operations Center will prompt you to either cancel the distribution or confirm that you want to overwrite the existing template.

Related Topics
- Viewing Configuration Templates Using Operations Center
- Configuring Devices Using Operations Center

Monitoring Your Network Using Operations Center

After viewing the various dashboards available in the Operations Center, you can then take a closer look at what is going on in your network. Specifically, you can monitor:

- The devices that belong to your network.
- The Prime Infrastructure servers that manage those devices.
- The alarms, events and other incidents that have taken place in your network.
- The clients and users configured to use your network.

The following related topics cover these items in more detail.

Related Topics
- Monitoring Devices Using Operations Center
- Using Virtual Domains With Operations Center
- Managing and Monitoring Prime Infrastructure Servers Using Operations Center
- Viewing the Prime Infrastructure Server Status Summary in Operations Center
- Viewing Prime Infrastructure Server Software Updates in Operations Center
- Viewing Prime Infrastructure Server Reachability History in Operations Center
- Viewing Alarms and Events Using Operations Center
- Viewing Clients and Users Using Operations Center
- Cross-Launching Prime Infrastructure Using Operations Center
- Viewing the Operations Center Dashboards

Monitoring Devices Using Operations Center

Select Monitor > Managed Elements > Network Devices to open the Network Devices page in Operations Center. From here, you can view information for every device that belongs to your network that a Prime Infrastructure instance is managing. This information includes the device’s hostname/IP address, its current reachability status, and the last time inventory data was successfully collected from that device.
When you first open the Network Devices page, every network device is displayed. To refine the devices displayed, do one of the following:

- From the Device Group pane, select the desired device type, location, or user-defined group.
- Apply a custom filter or select one of the predefined filters from the Show drop-down list. Operations Center provides a custom filter that allows you to view duplicate devices across your managed instances. For details on how to use filters, see the related topic “Performing a Quick Filter”.
- Search for a particular device. For details, see the related topic “Search Methods”.

If you delete a device from the Operations Center Network Devices page, the device is also deleted from all the managed Prime Infrastructure instances monitoring that device.

Related Topics
- Performing a Quick Filter
- Search Methods
- Monitoring Your Network Using Operations Center
- Using Virtual Domains With Operations Center

**Using Virtual Domains With Operations Center**

As explained in “Controlling User Access” in Related Topics, this feature provides an Operations Center administrator the ability to define a virtual domain on managed Prime Infrastructure instances. The Virtual Domains page will be modified to give Operations Center administrators visibility to each virtual domain defined under a managed Prime Infrastructure instance. The list of domains will be consolidated and displayed in the Operations Center.

From the Operations Center, you can view all the virtual domains available in all of the Prime Infrastructure instances that Operations Center is managing.

You can also create or edit virtual domains from Operations Center itself. If the same virtual domain is active in multiple Prime Infrastructure instances, Operations Center displays the virtual domain once, with data aggregated from all the active virtual domains with the same name on all the managed Prime Infrastructure instances.

You can create virtual domain only if an instance is present or it is in reachable state. The Number of network elements in Virtual Domains is limited when compared to that of Prime Infrastructure, since the Virtual Domain shows only managed network elements.

Note that any virtual domain you create using Operations Center will be replicated across all the instances of Prime Infrastructure that Operations Center manages, and if selected network elements are not present in particular instances, an empty virtual domain will be created.

Creating and editing virtual domains from within Operations Center works the same way as creating and editing virtual domains in a single instance of Prime Infrastructure. For details on adding, editing and viewing virtual domains, see “Using Virtual Domains to Control Access” in Related Topics.

Related Topics
- Controlling User Access
- Using Virtual Domains to Control Access
- Monitoring Your Network Using Operations Center
- Monitoring Devices Using Operations Center
• Managing and Monitoring Prime Infrastructure Servers Using Operations Center
• Creating Existing Virtual Domain in New Instances
• Maximum Virtual Domains Supported in Operations Center

Maximum Virtual Domains Supported in Operations Center

We recommend you use Express OVA for Operations Center. For Express OVA, the maximum number of Virtual Domains supported in Operations Center is 100 (Including Virtual Domains in Prime Infrastructure instances). Also you have an option to increase CPU and Memory of Operations Center server to higher configuration based on number of Virtual Domains supported. For more understanding, please refer Cisco Prime Infrastructure 3.1 Quick Start Guide, for metrics of hardware profiles and the respective number of Virtual Domains supported.

Related Topics
• Using Virtual Domains With Operations Center
• Creating Existing Virtual Domain in New Instances

Creating Existing Virtual Domain in New Instances

In Operations Center, if you want to create the existing virtual domain in new instances, follow these steps:

Step 1 Choose Administration > Users > Virtual Domains.
Step 2 From the Virtual Domains sidebar menu, click an existing virtual domain which you want to create in new instance.
Step 3 Click Managed Servers tab.
Step 4 Click Distribute to All Servers.
Step 5 Click Submit.

Related Topics
• Controlling User Access
• Using Virtual Domains With Operations Center
• Maximum Virtual Domains Supported in Operations Center

Role Based Access Control Support in Operations Center

The Role Based Access Control (RBAC) support in Operations Center allows a collection of devices from multiple managed instances to be associated with a user via virtual domains. This feature enables to assign privileges such as accessing Monitor and Manage server page, adding, modifying or deleting managed instances and providing Nbi privilege to generate reports and populate certain dashlets, to a specific user.

Follow these steps to enable RBAC in the Operations Center:
Step 1  Log in to Prime Infrastructure as an administrator.
Step 2  Choose Administration > Users > Users, Roles & AAA > User Groups.
Step 3  Click a group name to which RBAC is to be provided.
Step 4  Click Task Permissions tab.
Step 5  Check the following check boxes under Operations Center Tasks:
   - Monitor and Manage Servers Page Access
   - Administrative Privileges under Manage and Monitor Server Pages
   - Nbi Security Exception.
   These options are enabled by default for admin and super users.
Step 6  Click Save.

Related Topics
   - Controlling User Access
   - Using Virtual Domains With Operations Center
   - Maximum Virtual Domains Supported in Operations Center

Managing and Monitoring Prime Infrastructure Servers Using Operations Center

Select Monitor > Monitoring Tools > Manage and Monitor Servers to open the Manage and Monitor Servers page. From here, you can:
   - Add new Prime Infrastructure servers (up to the license limit).
   - Edit, delete, activate, and deactivate current Prime Infrastructure servers.
   - View each servers’ reachability, network latency, CPU utilization, memory utilization, software update status and secondary server details (if it is configured), license count, and alarms generated for the Prime Infrastructure instances.
   - Determine whether any servers are down.
   - View alarms and events.
   - Cross-launch into individual Prime Infrastructure instances.
   - See if any backup servers are running. Administrators can use the Prime Infrastructure High Availability (HA) framework to configure a backup Prime Infrastructure server to automatically come online and take over operations for the associated primary server when it goes down. For more information on Prime Infrastructure’s HA framework, see “Configuring High Availability” in Related Topics. Administrators should be sure to follow the restrictions on use of HA with Operations Center given in “Before You Begin Setting Up High Availability”.

Aside from a server’s reachability status, there are three server metrics you should focus on:
   - Network latency
   - CPU utilization
   - Memory utilization.
If a server has a network latency figure that exceeds one second, or it has a CPU or memory utilization percentage greater than 80%, the chances are good that an issue exists with that server.

If a server’s status is listed as “unreachable”, a “?” icon will appear next to the reachability status message. Hover your mouse cursor over the icon to see a popup message giving possible causes for the server’s status (for example, server cannot be pinged, API response (latency) is too slow and SSO is not setup properly).

Related Topics
- Configuring High Availability
- Before You Begin Setting Up High Availability
- Monitoring Your Network Using Operations Center
- Using Virtual Domains With Operations Center
- Viewing the Prime Infrastructure Server Status Summary in Operations Center

**Viewing the Prime Infrastructure Server Status Summary in Operations Center**

Use the Server Status Summary to view the current status of your Prime Infrastructure servers without leaving the dashboard or page you have open. To open it, place your cursor over any portion of the Server Status area at the top of the Operations Center’s main page. From here, you can quickly determine if any of your servers are currently down. You can also launch a separate Prime Infrastructure instance for the selected server.

Related Topics
- Monitoring Your Network Using Operations Center
- Cross-Launching Prime Infrastructure Using Operations Center
Viewing Prime Infrastructure Server Software Updates in Operations Center

You can quickly view the list of software updates that have been applied to any Prime Infrastructure server managed by Operations Center.

**Step 1** Select Monitor > Monitoring Tools > Manage and Monitor Servers. Operations Center displays the list of Prime Infrastructure servers it manages.

**Step 2** Select one of the managed servers. The page displays summary status for that server.

**Step 3** Click the **Software Updates** tab at the bottom of the page. Operations Center displays the list of software updates applied to the selected Prime Infrastructure server.

---

**Related Topics**
- Monitoring Your Network Using Operations Center
- Cross-Launching Prime Infrastructure Using Operations Center

Viewing Prime Infrastructure Server Reachability History in Operations Center

You can quickly view the reachability history for any Prime Infrastructure server managed by Operations Center.

**Step 1** Select Monitor > Monitoring Tools > Manage and Monitor Servers. Operations Center displays the list of Prime Infrastructure servers it manages.

**Step 2** Select one of the managed servers. The page displays summary status for that server.

**Step 3** Click the **Reachability History** tab at the bottom of the page. Operations Center displays a list of recent changes in reachability for the selected Prime Infrastructure server.

---

**Related Topics**
- Monitoring Your Network Using Operations Center
- Cross-Launching Prime Infrastructure Using Operations Center
Viewing Alarms and Events Using Operations Center

Select Monitor > Monitoring Tools > Alarms and Events to open the Alarms and Events page. From here, you can view a comprehensive listing of your network's alarms, events, and syslog messages. With one or multiple alarms selected, you can also determine whether those alarms have been acknowledged, add a note that describes them in more detail, or delete them from the page.

The Alarm Summary displays an aggregated count of critical, major, and minor alarms from the managed Prime Infrastructure instances.

To refine the alarms, events, and syslog messages displayed here, do one of the following:

- From the Device Group pane, select the desired device type, location, or user-defined group.
- Apply a custom filter or select one of the predefined filters from the Show drop-down list. For details on how to use filters, see the related topic “Performing a Quick Filter”.
- Search for a particular alarm or event. For details, see the related topic “Search Methods”.
- Hover your cursor on the Alarm Browser screen to display the aggregated count of alarms for the managed Prime Infrastructure instances. You can also acknowledge, annotate, and delete alarms; that action is duplicated on the respective Prime Infrastructure instance.

Related Topics

- Performing a Quick Filter
- Search Methods
- Monitoring Your Network Using Operations Center
- Viewing Clients and Users Using Operations Center
Viewing Clients and Users Using Operations Center

Select Monitor > Monitoring Tools > Clients and Users to open the Clients and Users page, which contains the aggregated clients of all managed Prime Infrastructure instances. From here, you can view information for the clients configured on your network, such as a client’s MAC address, the user associated with the client, and the name of the device that hosts the client. By clicking a client’s corresponding radio button, you can access even more detailed information for that client at the bottom of the Clients and Users page. To refine the list of clients displayed here, do one of the following:

- Apply a custom filter or select one of the predefined filters from the Show drop-down list. For details on how to use filters, see the related topic “Performing a Quick Filter”.
- Search for a particular client. For details, see the related topic “Search Methods”.

Related Topics
- Performing a Quick Filter
- Search Methods
- Monitoring Your Network Using Operations Center

Cross-Launching Prime Infrastructure Using Operations Center

A common element in the Operations Center’s four Monitor pages is the Prime Server column, which indicates the Prime Infrastructure server associated with any given device, alarm, event, client, or user. By clicking the corresponding link in any of the Monitor pages or the Server Status summary, you can launch a separate Prime Infrastructure instance to perform the necessary management tasks without closing the Operations Center.

Related Topics
- Monitoring Your Network Using Operations Center

Running Reports With Operations Center

In addition to the Operations Center dashboards and monitor pages, Operations Center provides a subset of Prime Infrastructure reports that combine network management and performance data across all the managed instances of Prime Infrastructure. If you are using Operations Center to segment and rationalize your management of a global network, these specialized versions of the standard reports can help get a closer look at your network as a whole, help you monitor health across the globe, and troubleshoot emergent issues.

The Operations Center reports contain aggregated data from all of the managed Prime Infrastructure instances. If you want to restrict this aggregation to a subset of the managed instances, the best ways to do this are to:

- Temporarily deactivate those Prime Infrastructure managed instances whose data you do not want included in the aggregated Operations Center report data. You can do this by selecting Monitor > Monitoring Tools > Manage and Monitor Servers and choosing to deactivate the servers you want to ignore.
- Use virtual domains to restrict the data the instances in which you are interested. For details, see “Using Virtual Domains With Operations Center” in Related Topics.
Except for aggregating data across managed instances, Operations Center reports generation works the same way as in Prime Infrastructure. For more information about Prime Infrastructure reports and how to generate them, see “Managing Reports” in Related Topics.

Related Topics
- Generating Reports
- Viewing the Operations Center Dashboards
- Monitoring Your Network Using Operations Center
- Using Virtual Domains With Operations Center
- Viewing Alarms and Events Using Operations Center
- Viewing Clients and Users Using Operations Center
- Operations Center FAQs

Operations Center FAQs

Q. What are the system requirements for Operations Center, and what OVA size should I use?
A. Operations Center requires the Standard OVA to manage up to 100 virtual domains. To manage more virtual domains, you must use a bigger OVA. See the full list of system requirements in the Scaling for Operations Center section in the Cisco Prime Infrastructure 3.1 Quick Start Guide.

Q. How does the licensing work in Operations Center?
A. Prior to release 3.1, there were two license files that had to be applied in Operations Center (a base license and an incremental license). Starting with version 3.1, you apply a single license file to transform the Prime Infrastructure instance to an Operations Center instance and to indicate how many instances you can manage in Operations Center.

After applying the license, log out and log back in for the changes to take affect.

Q. What communication ports must be opened between Operations Center and its managed instances?
A. You must enable Single Sign On (SSO) when you set up Operations Center. The SSO server and its managed instances are configured as the SSO client. SSO requires two ports to be open:
- 443 (HTTPS)
- 8082 (used for setting up SSL certificate).

Q. Why does the number of alarms in the Alarm Summary and the total alarm count differ in Operations Center and the managed instances?
A. You might have customized settings differently for the Operations Center and the managed instances. Check the following on both Operations Center and the managed instances to ensure they have the same settings:
- User Preferences—Click your login name in the top right-hand corner, then click My Preferences. Make sure the settings under Alarms are the same in Operations Center and the managed instances.
System Settings—Choose **Administration > Settings > System Settings**, then click **Alarms and Events**. Make sure that all the settings under Alarm Display Options are the same in Operations Center and the managed instances. By default, Prime Infrastructure and Operations Center hide acknowledged and cleared alarms, but you can choose to display them.

For more information, see Customizing the Alarm Summary in the *Cisco Prime Infrastructure 3.1 User Guide*.

**Q.** Why does the number of aggregated events and syslogs differ in Operations Center and managed instances?

**A.** Events and syslogs are constantly changing on managed instances. (If you click the **Refresh** button every 5 seconds, you can see the constant changes.) Because of the time it takes to update the corresponding information in Operations Center, these two numbers might not always be in sync. You should not compare the number displayed in the individual managed instances with the number displayed in Operations Center. The information displayed in the managed instances is more current than that displayed in the Operations Center.

**Q.** Why can’t I go directly to the Events page?

**A.** We will fix this issue in a future release. (See CSCui47865 for details.) To workaround this issue, on the Alarms page that is displayed, click the **Events** tab, then click **Refresh** to view the events data.

**Q.** Why does cross launching from Network Devices page, in some cases, display multiple devices instead of filtering on the selected device?

**A.** This is known limitation within Operations Center and is likely due to the similarity of device names on your managed instances.

**Q.** Why are there discrepancies in the report values generated between Operations Center and Prime Infrastructure?

**A.** Because of the differences in how the values are generated for Operations Center and Prime Infrastructure, minor discrepancies are expected. Prime Infrastructure generates values using fractional values. Operations Center aggregates these values using a set of rounded numbers. See CSCui29279 for details.

**Q.** Does Operations Center support third-party devices?

**A.** No. Because third-party devices are queried directly, there is not a corresponding NBI API to retrieve the data.

**Q.** From the Network Device Summary dashlet, why can’t I cross-launch to my third party APs?

**A.** This is a known issue. None of the third party APs are displayed.

**Q.** How do you enable GZip compression for reports?

**A.** To enable GZip compression in Operations Center go to **Administration > Settings > System Settings > General > Report**, click **Enable Compression**, then click **Save**.

**Q.** In Operations Center, why am I unable to cross-launch a managed instance and filter on my sylogs from the **Monitor > Monitoring Tools > Alarms and Events > Syslogs** tab?

**A.** Prime Infrastructure does not support filtering by instanceId for Syslogs. Therefore, Operations Center does not support filtering on Syslogs when cross launching to a managed instance.
Q. Why do Virtual Domains work incorrectly in Firefox version ESR 17.0.6?
A. You need to change the default character encoding scheme to Western(ISO-8859-1). By default, the character encoding is set to UTF8 in Firefox ESR 17.0.6. After you change the setting, refresh the browser.

Q. Why does the Current Associated Wired Clients table look different in Operations Center and Prime Infrastructure?
A. The Operations Center table has fixed columns, while Prime Infrastructure has customizable columns.

Q. Why is there a discrepancy in the VLAN ID and Association ID on the Clients and Users page between Operations Center and the managed instances?
A. This data changes frequently. As a result, the managed instances data may have already changed before the Operations Center was updated.

Q. Why is there a discrepancy in CPU Utilization and Memory Utilization fields for Autonomous AP on the device details page between Operations Center and the managed instances?
A. These fields change very quickly. Operations Center collects, aggregates, and then displays the data from the managed instances. Because of the time it takes to update this information in Operations Center, the data might not always be in sync. The information displayed in the managed instances is more current than that displayed in the Operations Center.

Q. Why does the network devices count (between Operations Center and managed instances) shown in the Network Devices table not match when someone tries to add them to a virtual domain?
A. In Prime Infrastructure, when you are adding a device to a virtual domain, you see all devices, even devices that cannot be added due to an incomplete inventory collection. In Operations Center, devices that cannot be added to a virtual domain are not displayed. See CSCuu41360 for details.

Q. Why do some managed instances keep going into Unreachable state?
A. This might occur if you initiate multiple concurrent cross-launches to the managed instances. This creates many SSO sessions for the managed instances, which might cause a session limit error and make the managed instance unreachable in Operations Center.

Q. Does Operations Center support High Availability (HA)?
A. HA is supported in both aspects:
   - HA on managed instances of Prime Infrastructure: Any and all of the Prime Infrastructure instances that you manage using Operations Center can have HA set up. Operations Center automatically detects the secondary server for each Prime Infrastructure instance that has HA set up. If the primary server in such setups goes down, Operations Center will automatically re-route all calls to the secondary server. It will also indicate the status of these instances by marking them as “Backup” on the Operations Center Manage & Monitor Servers page.
   - HA on the Operations Center instance: This is supported starting with version 3.1. You can specify a secondary server for Operations Center, which will be automatically activated when the primary instance goes down. Follow these steps to enable HA on Operations Center (for more details on each of these steps, see the Setting Up Operations Center):
     1. Set up two servers. These will serve as the primary and secondary HA Operations Center servers.
2. Enable Operations Center on the primary server and configure a Virtual IP on the primary server.

3. Log out from the primary Operations Center server and then log back in using the Virtual IP you configured.

4. Configure the primary Operations Center server as the primary SSO server, using the Virtual IP.

5. On each of your managed Prime Infrastructure instances, specify the primary Operations Center server as the primary SSO server, using the Virtual IP.

6. Add each of your managed Prime Infrastructure instances to the Operations Center server. Operations Center will fetch all data from the instances.

7. Shut down the primary Operations Center server and log in to the secondary server. The secondary server will operate as an Operations Center server and will fetch all data from the managed instances.

Q. What are the system requirements for Operations Center? Which size OVA should I use?

A. As of version 3.1, Operations Center requires (at a minimum) the Express OVA size with at least the following system specifications: 4 CPUs, 12GB Memory, 300GB Hard Disk. With this setup, Operations Center can manage up to 100 Virtual Domains, and up to 10 managed instances. You must choose a larger OVA to manage more virtual domains. For Operations Center to work properly, your network must support at least 250 kbps of bandwidth and latency of no more than 5 milliseconds between the Operations Center server and the managed instances.

A. How do you disable auto-logout in Operations Center?

A. To disable auto log out:

1. Click your login name in the top right-hand corner, then click My Preferences.
2. Under User Idle Timeout, uncheck Logout idle user, then click Save.
3. Choose Administration > Settings > System Settings > Server, then under Global Idle Timeout, uncheck Logout all idle users, then click Save.

Q. How do you set up Single-Sign-On (SSO) in Operations Center?

A. You must set up Single-Sign-On (SSO) so that Operations Center acts as the SSO server and the managed instances act as the SSO clients.

As of version 3.1, SSO can be configured automatically. Once you have configured SSO on the Operations Center server and applied the Operations Center license file, you can choose to configure SSO automatically on each managed instance as you add it using the Manage & Monitor Servers page, by checking the “Enable Single-Sign-On Automatically” checkbox.

If need be, you can also set up SSO manually, as explained in the following steps:

In Operations Center:

1. Select Administration > Users > Users, Roles & AAA, then select SSO Servers.
2. Choose Select a command > Add SSO Server, then click Go.
3. Complete the required fields, then click OK.
4. From the left-hand menu, select AAA Mode Settings.
5. Click SSO, then click Save.
In each managed instance:
1. Select Administration > Users > Users, Roles & AAA, then select SSO Servers.
2. Choose Select a command > Add SSO Server, then click Go.
3. Enter the IP address of the Operations Center server, then click OK.
4. From the left-hand menu, select AAA Mode Settings.
5. Click SSO, then click Save.

To ensure that SSO is working properly, log in to Operations Center, open a new browser tab and access one of your managed instances. If you are automatically logged into your Prime Infrastructure instance without having to re-authenticate, then SSO is working as expected.

Q. Does Operations Center support TACACS?
A. Yes. To set up TACACS or another central authentication server in Operations Center, follow these steps:
1. Select Administration > Users > Users, Roles & AAA, then select TACACS+ Servers from left-hand menu
2. From the Select a command dropdown menu, select Add TACACS+ Server, then click Go.
3. Complete the required fields, then click OK.
4. From the left-hand menu, select SSO Server Settings.
5. Click TACACS+, then click Save.

Q. How do I avoid a single point of failure with Operations Center?
A. You can do this by configuring a second Prime Infrastructure instance as an SSO server. Ensure that it contains all the TACACS details (if applicable). Specify this server as the second SSO server for all your managed instances. If your Operations Center server goes down, the Prime Infrastructure instances will reroute to this instance to authenticate users. Also, starting with version 3.1, you can set up High Availability (HA) for Operations Center itself, by specifying primary and secondary HA servers.

Q. What is the maximum number of supported instances in Operations Center?
A. Operations Center currently supports up to 10 managed instances. This is not a hard limit. You can add more managed instances as long as your license allows for them. However, Cisco recommends that you observe the 10-instance limit for performance reasons. Operations Center must wait for responses from all its managed instances before aggregating and displaying their data. The more instances you add to Operations Center, the more data it needs to process and the slower it becomes. Adding more instances also increases the likelihood that one or more of the managed instances will serve as a bottleneck.

Q. How does Operations Center’s license count work with respect to Prime Infrastructure instances that have a secondary High Availability (HA) server setup?
A. Secondary HA servers are not accounted for as part of your license count when adding your managed instances to Operations Center. In other words if your Operations Center license allows for management of three instances, that means three instances with or without HA. Hence, you will need to specify a count of “3” for your L-PI2X-OPRCTR-1 license.
Q. When Operations Center is managing multiple Prime Infrastructure instances, do we lose GUI or CLI access to those individual instances?

A. No, but remember that Operations Center acts as the Single-Sign-On (SSO) server and its managed Prime Infrastructure instances act as SSO clients. So you will only be able to login to the GUI of your Prime Infrastructure instances with credentials defined in Operations Center. You will not be able to login to any of the Prime Infrastructure instances with credentials defined locally on that instance. Operations Center does not affect CLI access to your Prime Infrastructure instances in any way.

Q. What is the impact to managed Prime Infrastructure instances if an Operations Center server without High Availability (HA) goes down?

A. If you don’t have HA set up with Operations Center and your Operations Center server goes down, the individual Prime Infrastructure instances will fallback to “Local Authentication” mode and will allow you to login using their local credentials. Starting with version 3.1, Prime Infrastructure instances can also fallback to a centralized authentication server (such as TACACS) if one is specified.
Configuring Devices

- Configuring Network Devices
- Using Templates to Configure Devices
- Configuring Wireless Devices
- Creating Controller Configuration Groups
- Configuring Wireless Technologies
- Scheduling Configuration Tasks
- Auditing Device Configurations to Ensure Compliance
- Configuring Plug and Play
Configuring Network Devices

From the **Configuration > Network > Network Devices** page, you can view all devices and device configuration information. The Network Devices page contains configuration functions as described in **Table 25-1**.

**Table 25-1 Configuration > Network > Network Devices Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Location in Configuration &gt; Network &gt; Network Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage devices</td>
<td>You can add, edit, delete, sync, and export devices, add and delete devices from groups and sites, and perform a bulk import.</td>
<td>Buttons are located across the top of the page.</td>
</tr>
<tr>
<td>View basic device information and collection status</td>
<td>View basic device information such as reachability status, IP address, device type, and collection status.</td>
<td>Click the icon next to the IP Address to access the 360° view for that device. For controllers, click the arrow to launch the controller web UI. Hover your mouse cursor over the Reachability cell to view the status. Click the icon in the Last Inventory Collection cell to view errors related to the inventory collection.</td>
</tr>
<tr>
<td>Manage device groups</td>
<td>By default, Cisco Prime Infrastructure creates dynamic device groups and assigns devices to the appropriate Device Type folder. You can create new device groups that appear under the User Defined folder.</td>
<td>Displayed in the left pane of the page.</td>
</tr>
</tbody>
</table>
### Table 25-1  **Configuration > Network > Network Devices Tasks (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Location in Configuration &gt; Network &gt; Network Devices</th>
</tr>
</thead>
</table>
| Add devices to site groups               | After you set up a site group profile, you can add devices to it. To add devices to site groups in Network Devices page, add them to Group and then select site group. To add devices to site maps, go to the Maps > Site Map.  

**Note** A device can belong to one site group hierarchy only.  

**Note** The devices added to a site group on this page are not added in the Maps > Site Map page. Similarly, the devices added in the Site Map Design page are not added to site groups on this page. | Groups & Sites button located at the top of the page.                                                                                                                   |
| Modify the Admin state of devices        | You can select one of the following admin state options for devices:  

- **Set to Maintenance State**—Specifies no polling, device inventory collection, or alarms. The Last Inventory Collection status becomes In Service Maintenance.  

- **Set to Managed State**—Prime Infrastructure manages the device, collects inventory, and processes alarms. The Last Inventory Collection status changes from In Service Maintenance to Synchronizing, to Completed state. | Admin State button located at the top of the page.                                                                                                                     |
| View device details                      | View device details such as memory, port, environment, and interface information.                                                                                                                           | Click on a Device Name to view the detailed configuration information for that device.                                                                                   |
| Create and deploy configuration templates | You can configure device features on the selected device. You can also view the list of applied and scheduled feature templates that were deployed to the device.                                            | Click on a Device Name, then click the Configuration tab.                                                                                                                 |
| View device configurations               | View archived configurations, schedule configuration rollbacks, and schedule archive collections.                                                                                                         | Click on a Device Name, then click the Configuration Archives tab.                                                                                                          |
| View software images                     | You can view the recommended software image for a single device, and then import or distribute that image.                                                                                            | Click on a Device Name, then click the Image tab.  

Scroll down to Recommended Images to view the recommended image for the device that you selected. Prime Infrastructure gathers the recommended images from both Cisco.com and the local repository. |
Table 25-1  Configuration > Network > Network Devices Tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Location in Configuration &gt; Network &gt; Network Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>View interface details</td>
<td>You can view the description, admin status, and</td>
<td>Click on a Device Name, click the Configuration tab, then in the left frame, click Interfaces to view the interface details.</td>
</tr>
<tr>
<td></td>
<td>operational status of the interface.</td>
<td></td>
</tr>
<tr>
<td>View and modify TrustSec</td>
<td>You can view and modify the TrustSec configuration</td>
<td>Click on a Device Name, click the Configuration tab, then in the left frame, click Security &gt; TrustSec &gt; Wired 802_1x.</td>
</tr>
<tr>
<td>configuration</td>
<td>of a TrustSec-based device.</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Network Devices
- Using Templates to Configure Devices
- Configuring Wireless Devices
- Creating Controller Configuration Groups
- Configuring Wireless Technologies
- Scheduling Configuration Tasks
- Auditing Device Configurations to Ensure Compliance
- Configuring Plug and Play
Using Templates to Configure Devices

You can use Cisco Prime Infrastructure configuration templates to design the set of device configurations that you need to set up the devices in a branch. When you have a site, office, or branch that uses a similar set of devices and configurations, you can use configuration templates to build a generic configuration that you can apply to one or more devices in the branch. You can also use configuration templates when you have a new branch and want to quickly and accurately set up common configurations on the devices in the branch. Altering configurations across a large number of devices can be tedious and time-consuming, and templates save you time by applying the necessary configurations and ensuring consistency across devices.

Related Topics
- Guidelines for Planning Your Network Design
- Creating Feature-Level Configuration Templates
- Features and Technologies Templates
- CLI Templates
- Composite Templates
- Feature Templates
- My Tags
- Controller Templates
- Shared Policy Objects
- Configuration Groups
- WLAN Controller Configuration Groups
- Wireless Configuration Templates
- Creating Switch Location Templates
- Deploying Templates

Guidelines for Planning Your Network Design

Consider the following factors when using the Prime Infrastructure to create reusable design patterns to simplify device configurations. When you plan your network design and then create templates based on that design, you can increase operational efficiency, reduce configuration errors, and improve compliance to standards and best practices:
• What is the size of your network?
• How diverse are the devices and services that you support?
• How many network designers do you have?
• What degree of precision do you need in controlling your network?

If you have a small network with only one or two designers and not much variation among device configurations, you could start by copying all CLI configurations you know are “good” into a set of configuration and monitoring templates, then create a composite template that contains these templates.

If you have a large network with many different devices, try to identify the configurations you can standardize. Creating feature and technology templates as exceptions to these standards allows you to turn features on and off as needed.

Related Topics
• Creating Feature-Level Configuration Templates
• Composite Templates
• Shared Policy Objects
• WLAN Controller Configuration Groups
• Wireless Configuration Templates
• Creating Switch Location Templates

Creating Feature-Level Configuration Templates

Cisco Prime Infrastructure provides the following types of feature-level configuration templates:
• Features and technologies templates—Configurations that are specific to a feature or technology in a device’s configuration.
• CLI templates—User-defined templates that are created based on your own parameters. CLI templates allow you to choose the elements in the configurations. Prime Infrastructure provides variables that you replace with actual values and logic statements. You can also import templates from the Cisco Prime LAN Management System.
• Composite templates—Two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices.

If the Save as New Template button is grayed out for the existing templates, do the following:
• Export the existing template by clicking the Export icon at the top right of the FlexConnect template page.
• Open the exported file using any HTML/text editor.
• Find and replace the name of the template.
• Import the template into the FlexConnect folder.
• Make changes to the settings and save.

Related Topics
• Features and Technologies Templates
Features and Technologies Templates

Features and Technologies templates are templates that are based on device configuration and that focus on specific features or technologies in a device’s configuration.

When you add a device to Prime Infrastructure, Prime Infrastructure gathers the device configuration for the model you added. Prime Infrastructure does not support every configurable option for all device types. If Prime Infrastructure does not have a Features and Technologies template for the specific feature or parameter that you want to configure, create a CLI template.

Features and Technologies templates simplify the deployment of configuration changes. For example, you can create an SNMP Features and Technologies template and then quickly apply it to devices you specify. You can also add this SNMP template to a composite template. Then later, when you update the SNMP template, the composite template in which the SNMP template is contained automatically has your latest changes.

To view the list of Features and Technologies templates, choose Configuration > Templates > Features & Technologies > Features and Technologies.

Related Topics
- Features and Technologies Field Descriptions
- Creating Features and Technologies Templates
- Deployment Flow for Configuration Templates Using the Wizard

Creating Features and Technologies Templates

To create Features and Templates, follow these steps:

**Step 1** Choose Configuration > Templates > Features and Technologies.

**Step 2** In the Features and Technologies menu on the left, choose a template type to create.

**Step 3** Complete the fields for that template.

If you are creating a feature template that applies only to a particular device type, the Device Type field lists only the applicable device type, and you cannot change the selection. Specifying a device type helps you to prevent a mismatch; that is, you cannot create a configuration and apply the configuration to a wrong device.

**Step 4** Click Save as New Template. After you save the template, control gets redirected to the saved template from where you can deploy it to your devices.

**Step 5** To verify the status of a template deployment, choose Administration > Dashboard > Jobs Dashboard.
To modify the deployment parameters for any subsequent configuration template deployments, select a configuration job, then click **Edit Schedule**.

---

**Related Topics**
- Features and Technologies Field Descriptions
- Deployment Flow for Configuration Templates Using the Wizard

---

**Deployment Flow for Configuration Templates Using the Wizard**

**Note**
This deployment flow is not applicable for Controller based templates. For information on how to deploy Controller based templates, see the Deploying Templates section.

**Step 1** After you create a configuration template, click **Deploy**. The Deployment wizard page opens.

**Step 2** Select the devices on which you want to deploy the template, then click **Next** to choose the input values.

**Step 3** Select the ports on which you want to deploy the template, then click Next to choose the input values.

This option appears only if you have tagged the template as ports based, while creating the template.

**Step 4** In the **Input Values** tab, you can toggle between Form and CLI view.

**Step 5** After entering the necessary configuration values, click **Next** or click **CLI** to confirm the device and template configuration values.

**Step 6** Schedule the deployment job using **Schedule Deployment** tab, if required:
- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:
  - **Failure Policy**
    - **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
    - **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn’t undergo template deployment, “Not Attempted” message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
    - **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
    - **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

**Step 7** Click **Next** to view the job deployment summary.

**Step 8** On the Deployment Summary tab, you will see the CLI view for each of the device.

**Step 9** Click **Finish** to deploy the template.
Click **Job Status** in the pop-up dialog box to launch the **Job Dashboard** to view the status of the job.

---

**Related Topics**

- Creating Features and Technologies Templates

---

**CLI Templates**

CLI templates are a set of re-usable device configuration commands with the ability to parameterize select elements of the configuration as well as add control logic statements. This template is used to generate a device deployable configuration by replacing the parameterized elements (variables) with actual values and evaluating the control logic statements.

The following are the list of CLI templates:

- **System Templates - CLI**—You cannot delete a System Template, but you can modify and save it as a new template. In this page, you can import or export any template. You cannot import a template under the system defined folder. The Undeploy button is disabled in this page since the CLI templates do not have an option undeploy them.

- **CLI**—CLI is a set of re-usable device configuration commands with the ability to parameterize select elements of the configuration as well as add control logic statements. This template is used to generate a device deployable configuration by replacing the parameterized elements (variables) with actual values and evaluating the control logic statements.

To view the list of system CLI templates, choose **Configuration > Templates > Features and Technologies > CLI Templates**.

**Related Topics**

- Prerequisites for Creating CLI Templates
- Creating CLI Configuration Templates
- Creating CLI Configuration Templates from Copied Code
- Exporting a Template
- Importing a CLI Configuration Template
- Exporting CLI Variables
- Importing CLI Variables
- Example: Updating Passwords Using a CLI Template
- Example: Updating Passwords Using a CLI Template
- Example: Updating Passwords Using a CLI Template
- CLI Template Field Description

---

**Prerequisites for Creating CLI Templates**

Before you create a CLI template, you must:

- Have expert knowledge and understanding of the CLI and be able to write the CLI in Apache VTL.
- Understand to what devices the CLI you create can be applied.
• Understand the data types supported by Prime Infrastructure.
• Understand and be able to manually label configurations in the template.

Related Topics
• Variables and Data Types
• Apache Velocity Template Language

Creating CLI Configuration Templates

Use templates to define device parameters and settings, which you can later to a specified number of devices based on device type.

Before You Begin
Make sure that you have satisfied the prerequisites (see Prerequisites for Creating CLI Templates).

Step 1 Choose Configuration > Templates > Features and Technologies.

Step 2 Expand the CLI Templates folder, then click CLI.

Step 3 Complete the required fields in the Template Basic section.

Step 4 Click the Ports radio button, if you want to apply the template to a set of selected interfaces across selected devices.

The template will be tagged as port based template.

Step 5 In the Template Detail section, configure the following:

• Click the Add Variable tab. This allows you to specify a variable for which you will define a value when you apply the template. Click Add Row and enter the parameters for the new variable, then click Save.

or

Search for the global variable in the Add Global Variable search box by entering the first few characters of the global variable name and choose the desired global variable you want to apply

• Enter the CLI information. In the CLI tab, you must enter code using Apache VTL.

• (Optional) To change the variables, click the Manage Variables icon, and then make your changes. Click Form View (a read-only view) to view the variables.

Step 6 Click Save As New Template, specify the folder in which you want to save the template, then click Save.

To duplicate a CLI template, expand the System Templates - CLI, hover your mouse cursor over the quick view picker icon next to CLI, and then click Duplicate.

Related Topics
• Variables and Data Types
• Managing Database Variables in CLI Templates
• Apache Velocity Template Language
• Using Validation Expression
• Adding Multi-line Commands
Variables and Data Types

You can use variables as placeholders to store values. The variables have names and data types. Table 26-1 lists data types that you can configure in the Manage Variables page.

Table 26-1 Data Types

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>Enables you to create a text box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.</td>
</tr>
<tr>
<td>Integer</td>
<td>Enables you to create a text box that accepts only numeric value. If you want to specify a range for the integer, expand the row and configure the Range From and To fields. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.</td>
</tr>
<tr>
<td>DB</td>
<td>Enables you to specify a database type.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>Enables you to create a text box that accepts only IPv4 addresses for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.</td>
</tr>
<tr>
<td>Drop-down</td>
<td>Enables you to create a list for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field (with a comma-separated value for multiple lists which appears in the UI).</td>
</tr>
<tr>
<td>Check box</td>
<td>Enables you to create a check box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field.</td>
</tr>
<tr>
<td>Radio Button</td>
<td>Enables you to create a radio button for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field.</td>
</tr>
<tr>
<td>Text Area</td>
<td>Enables you to create a text area which allows multiline values for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.</td>
</tr>
</tbody>
</table>

Managing Database Variables in CLI Templates

You can use database (DB) variables for the following reasons:

- DB variables are one of the data types in CLI templates. You can use the DB variables to generate device-specific commands.
- DB variables are predefined variables. To view the list of predefined DB variables, see the CLITemplateDbVariablesQuery.properties file in the following folder
  /opt/CSColumos/conf/ifm/template/inventoryTagsInTemplate.
- For example, SysObjectID, IPAddress, ProductSeries, ImageVersion are DB variables. When a device is added to Prime Infrastructure, the complete details of the device are collected in the DB variables. That is, the OID of the devices is collected in SysObjectID, product series in ProductSeries, image versions of the device in ImageVersion, and so on.
- Using the data collected by the DB variables, accurate commands can be generated to the device.
Chapter 26      Using Templates to Configure Devices

CLI Templates

You can select the DB variable in the Type field (using the Managed Variables page). Expand the name field and fill in the default value field with any of the DB variables which you want to use.

When a device is discovered and added to Prime Infrastructure, you can use the database values that were gathered during the inventory collection to create CLI templates.

For example, if you want to create a CLI template to shut down all interfaces in a branch, create a CLI template that contains the following commands:

```
#foreach ($interfaceName in $interfaceNameList)
  interface $interfaceName
  shutdown
#end
```

where $interfaceNameList is the database variable type whose value will be retrieved from the database. $interfaceNameList has a default value of IntfName. You need to create the interfaceNameList variable as DB data type (using the managed variable dialog box) and add set the default to IntfName. If you have not specified a default value, you can specify it when you apply the CLI template.

To populate interfaceNameList with the value from the database, you must create a properties file to capture the query string and save it in the /opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate folder.

To view the predefined DB variables go to the following path:

```
cd /opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate
```

After you create and apply the CLI template and the property file, the following CLI is configured on the devices. This output assumes that the device has two interfaces (Gigabitethernet0/1 and Gigabitethernet0/0):

```
interface GigabitEthernet0/0
shutdown
interface GigabitEthernet0/1
shutdown
```

**Note**
While it is possible to create a customized query using Enterprise JavaBeans Query Language (EJB QL), only advanced developers should attempt this. We recommend you use the variables defined in the CLITemplateDbVariablesQuery.properties file only.

Using Validation Expression

The values that you define in the Validation Expression are validated with the associated component value. For example, if you enter a default value and a validation expression value in the design flow, this will be validated during the design flow. That is, if the default value does not match with the entered value in the validation expression, you will encounter a get error at the design flow.

**Note**
The validation expression value works only for the string data type field.

Example:

Choose Configuration > Features and Technologies > CLI Templates > CLI > Manage Variables > Add Row. Choose string data type and then expand the row and configure the regular expression, which will not allow a space in that text box.

Enter the following expression in the validating expression field.

```
^\S+$
```
Default value (optional)—ncs
The value should match with regular expression in the validation expression field.)

Result:
Save the template, and then select a device. Try to enter a space in the text field. You will encounter a regular expression error.

Adding Multi-line Commands

To enter multi-line commands in the CLI Content area, use the following syntax:

<MLTCMD>First Line of Multiline Command
Second Line of Multiline Command
......
......
Last Line of Multiline Command</MLTCMD>

where:
- <MLTCMD> and </MLTCMD> tags are case-sensitive and must be entered as uppercase.
- The multi-line commands must be inserted between the <MLTCMD> and </MLTCMD> tags.
- Do not start this tag with a space.
- Do not use <MLTCMD> and </MLTCMD> in a single line.

Example 1:
<MLTCMD>banner motd ~ Welcome to Cisco. You are using Multi-line commands. ~</MLTCMD>

Example 2:
<MLTCMD>banner motd ~ ${message} ~</MLTCMD>

where message is a multi-line input variable.

Restrictions for Using Multi-line Banner Commands

You can use “banner file xyz” format as shown in the following example:

#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
(config)#parameter-map type webauth global
(config-params-parameter-map)# type webauth
(config-params-parameter-map)#banner file tftp://192.168.0.0/banner.txt
(config-params-parameter-map)#^Z
#more tftp://192.168.0.0/banner.txt
Disclaimer:
Usage of this wireless network is restricted to authorized users only.
Unauthorized access is strictly forbidden.
All accesses are logged and can be monitored.
#
Adding Enable Mode Commands

Use this syntax to add enable mode commands to your CLI templates:

```
#MODE_ENABLE
<<commands >>
#MODE_END_ENABLE
```

Adding Interactive Commands

An interactive command contains the input that must be entered following the execution of a command.

To enter an interactive command in the CLI Content area, use the following syntax:

```
CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question 2<R>command response 2
```

where <IQ> and <R> tag are case-sensitive and must be entered as uppercase.

For example:

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Combining Interactive Enable Mode Commands

Use this syntax to combine interactive Enable Mode commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

For example:

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Adding Interactive Multiline Commands

This is an example of an interactive command that contains multiple lines:

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
```
Creating CLI Configuration Templates from Copied Code

A quick way to create CLI configuration templates is to copy code from a command line configuration session, CLI script, or other stored set of configuration commands. Prime Infrastructure lets you turn all the CLI parameters in the copied CLI into template variables.

To create a CLI template variable from copied code:

1. Choose Configuration > Templates > Features and Technologies.
2. Expand the CLI Template folder, then click CLI.
3. In the CLI template, paste the copied code into the CLI Content field.
4. Select the text that is to be the variable name and click Manage Variables (the icon above the CLI Content field).
   
   You can use this same procedure to edit an existing variable created from copied code.
5. Fill out the required information, then click Save > Add.
6. To view the new variable, click Form View.

Related Topics
- Creating CLI Configuration Templates
- Deployment Flow for Configuration Templates Using the Wizard

Exporting a Template

If you have any CLI or Composite templates in any other Prime Infrastructure server, you can export them as an XML file and import them into your current Prime Infrastructure server.

1. Choose Configuration > Templates > Features and Technologies.
2. Expand the CLI Template or Composite Template folder.
3. Click System Templates - CLI or System Templates - Composite folder.
4. Select the template(s) that you want to export.
5. Click the Export icon at the top right of the CLI template page.
Related Topics
- Creating CLI Configuration Templates

## Importing a CLI Configuration Template

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Templates &gt; Features and Technologies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand the CLI Template folder, then hover your mouse cursor over the quick view picker icon next to CLI.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Show All Templates.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the Import icon at the top right of the CLI template page.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Select Templates to navigate to your file, then click OK.</td>
</tr>
</tbody>
</table>

Related Topics
- Creating CLI Configuration Templates

## Exporting CLI Variables

You can export the CLI variables into a CSV file while deploying a CLI configuration template. You can use the CSV file to make necessary changes in the variable configuration and import it into Prime Infrastructure at a later time.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Templates &gt; Features and Technologies &gt; CLI Templates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click System Templates - CLI.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the template whose variables you want to export.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Deploy.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select devices in Device Selection area.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click the Export icon at the top right of the Value Assignment area.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>

Exporting the variables without any data will export a blank file.

Related Topics
- Creating CLI Configuration Templates

## Importing CLI Variables

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Templates &gt; Features and Technologies &gt; CLI Templates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click System Templates - CLI.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the template whose variables you want to import.</td>
</tr>
</tbody>
</table>
Step 4: Click the Import icon at the top right of the CLI template page.

Step 5: Click OK.

Related Topics
- Creating CLI Configuration Templates

Example: Updating Passwords Using a CLI Template

You might want to update the password for network devices on a regular basis, once every six months. To make the changes in a rolling fashion, you plan to perform the operation once for two regions every three months.

In this example, there are four custom dynamic groups, one for each region based on the cities in every region: North Region, South Region, East Region, and West Region. You must update the enable password for all of the devices in the north and south region. After this is complete, you plan to set another job to occur for the West and East region devices to occur three months later.

Before You Begin
The devices in these regions must have an assigned location attribute.

Step 1
If the four groups, North Region, South Region, East Region, and West Region, have not been created:

a. Choose Inventory > Device Management > Network Devices, then hover your mouse cursor over User Defined and click Add SubGroup.

b. In the Create Sub-Group area, enter:
   - Group Name: North Region
   - Group Description: List of devices in the north region
   - Filter: Location > Contains > SJC-N

   To determine the location of a device, choose Inventory > Device Management > Network Devices > (gear icon) > Columns > Location.

   The devices for the new group appear under Device Work Center > User Defined > North.

c. Do the same for south, east, and west regions.

Step 2
To deploy the password template:

a. Choose Configuration > Templates > Features and Technologies > CLI Templates > System Templates-CLI.

b. Select the Enable Password-IOS template and click Deploy.

c. In the Device Selection area, open the User Defined groups and select the North Region and South Region groups.

d. In the Value Selection area, enter and confirm the new enable password, then click Apply.

e. In the Schedule area, enter a name for the job, the date and time to apply the new template (or click Now), then click OK.

Step 3
After the job has run, choose Administration > Jobs to view the status of the job.
Related Topics
- Creating CLI Configuration Templates

Deployment Flow for CLI Templates using the Wizard

Step 1  After creating the CLI template, click Deploy. The Deployment wizard page opens.
Step 2  Select the devices on which you want to deploy the template, then click Next to choose the input option.
Step 3  Select the mode in which you want to deploy the template. The options are Work Flow and Export/Import CSV.
Step 4  Click Work Flow option and click Next. See Step 6.
Step 5  Alternately, click Export/Import CSV option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.
   1. Uncheck the Do you want Optional Parameters check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
   2. Click Export CSV to download the CSV template to your local system.
   3. Enter the configuration values for each specific device in the downloaded CSV template.
   4. Click Import CSV to upload the updated CSV file. The input values automatically gets updated.
   5. Click Next to input values.
Step 6  In the Input Values tab, you can toggle between Form and CLI view.
Step 7  After entering the necessary configuration values, click Next or CLI to confirm the device and template configuration values.
Step 8  Schedule the deployment job in the Schedule Deployment tab, if required:
   • Create a meaningful deployment job name, then specify whether to run the now or in the future.
   • You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
   • You can configure the following job options:
     Failure Policy
     • Ignore failure and continue—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
     • Stop on failure—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn’t undergo template deployment, “Not Attempted” message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
     • Copy Running Config to Startup—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
     • Archive Config after deploy—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.
Step 9  Click Next to view the job deployment summary.
Step 10  On the Deployment Summary tab, you will see the CLI view for each of the device.
Step 11  Click Finish to deploy the template.
Composite Templates

Create a composite template if you have a collection of existing features or CLI templates that you want to apply collectively to devices. For example, when you deploy a branch, you need to specify the minimum configurations for the branch router. Creating a composite template allows you to create a set of required features that include:

- Feature templates for the Ethernet interface
- A CLI template for additional features you require

All of the templates that you create can be added to a single composite template, which aggregates all of the individual feature templates that you need for the branch router. You can then use this composite template to perform branch deployment operations and to replicate the configurations at other branches.

If you have multiple similar devices replicated across a branch, you can create and apply a master (golden) composite template for all of the devices in the branch. You can use this master composite template to:

- Simplify deployment and ensure consistency across your device configurations.
- Compare against an existing device configuration to determine if there are mismatches.
- Create new branches.

You can create the following Composite templates:

- System Templates - Composite
- Composite Template

To view the list of Features and Technologies templates, choose Configuration > Templates > Features & Technologies > Composite Templates.

Related Topics

- Creating Composite Templates
- Deployment Flow for Composite Templates Using the Wizard

Creating Composite Templates

**Step 1** Choose Configuration > Templates > Features & Technologies > Composite Templates > Composite Templates.

**Step 2** Provide the required information.

- From the Device Type drop-down list, choose the devices to which all of the templates contained in the composite template apply. For example, if your composite template contains one template that applies to Cisco 7200 Series routers and another that applies to all routers, choose the Cisco 7200 Series routers in the Device Type list.
  
  If a device type is dimmed, the template cannot be applied on that device type.

- In the Template Detail area, choose the templates to include in the composite template.
Using the arrows, put the templates in the composite in the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the interface template.

**Step 3** Click **Save as New Template**. After you save the template, and apply it to your devices.

**Related Topic**
- Deployment Flow for Composite Templates Using the Wizard

## Deployment Flow for Composite Templates Using the Wizard

**Step 1** Choose **Configuration > Templates > Features & Technologies > Composite Templates > Composite Templates**.

**Step 2** Enter the required information in the Template Basic section.

**Step 3** In the Template Detail section, choose the templates to include in the composite template, and click **Save as New Template**.

**Step 4** After creating the composite template, click **Deploy**. The Deployment wizard page opens.

**Step 5** Select the devices on which you want to deploy the template, then click **Next** to choose the input option.

**Step 6** Select the ports on which you want to deploy the template, then click Next to choose the input values. This option appears only if you have tagged the template as ports based, while creating the template.

**Step 7** Select the mode in which you want to deploy the template. The options are **Work flow** and **Export/Import CSV**.

**Step 8** Click **Work Flow** option and click **Next**. See Step 10.

**Step 9** Alternately, click **Export/Import CSV** option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.

  a. Uncheck the **Do you want Optional Parameters** check box, if you want to skip the optional fields while filling the configuration values in the CSV file.

  b. Click **Export CSV** to download the CSV template to your local system.

  c. Enter the configuration values for each specific device in the downloaded CSV template.

  d. Click **Import CSV** to upload the updated CSV file. The input values automatically gets updated.

  e. Click **Next** to input values.

**Step 10** In the **Input Values** tab, you can toggle between **Form** and **CLI** view. Configure the following in the Input Values tab:

  a. Select templates for a device from the navigation widget. To select templates, click the circle (T1, T2, T3, T4, T5 ...) in the upper right corner. If there are more than five templates, click three dots. The drop-down list will pop-up with all the available templates.

  b. Enter all the mandatory fields for each template, then click **Apply**.

     If the validation is successful, then the border of the circle around the selected template changes to green.

**Step 11** After entering the necessary configuration values, click **Next** or **CLI** to confirm the device and template configuration values.
Step 12 Schedule the deployment job in the **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:
  
  **Failure Policy**
  
  - **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  
  - **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn’t undergo template deployment, “Not Attempted” message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
  
  - **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
  
  - **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 13 Click **Next** to view the job deployment summary.

Step 14 On the **Deployment Summary** tab, you will see the CLI view for each of the device.

Step 15 Click **Finish** to deploy the template.

Step 16 Click **Job Status** in the pop-up dialog box to launch the **Job Dashboard** to view the status of the job.

---

**Related Topics**

- Composite Templates

---

## Feature Templates

Feature templates are configurations that are specific to a feature or technology in a device's configuration. Feature templates consist of system templates that are grouped based on device configuration.

Feature templates are system defined. You cannot delete a Feature Template, but you can modify and save it as a new template.

To access the Feature Templates page, choose **Configuration > Templates > Features & Technologies > Feature Templates**.

You can create the following Feature templates:

- IWAN
- NFV
- Router Security
My Tags

You can label a set of templates by providing an intuitive name to tag the templates. After you create a tagged template, the template is listed under the My Tags folder. Tagging a configuration template helps you:

- Search a template using the tag name in the search field
- Use the tagged template as a reference to configure more devices

To access the Feature Templates page, choose Configuration > Templates > Features & Technologies > My Tags.

Related Topics
- Tagging a New Configuration Template
- Tagging an Existing Template
- Associating a Tag With Multiple Templates

Tagging a New Configuration Template

To tag a new configuration template and publish the tagged template, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configuration &gt; Templates &gt; Features &amp; Technologies.</td>
</tr>
<tr>
<td>2</td>
<td>Expand the Features and Technologies folder, choose an appropriate subfolder, and then choose a template type.</td>
</tr>
<tr>
<td>3</td>
<td>Complete the required fields, enter a tag name in the Tags field, then click Save as New Template.</td>
</tr>
</tbody>
</table>

Related Topics
- My Tags
- Tagging an Existing Template
- Associating a Tag With Multiple Templates

Tagging an Existing Template

To tag an existing template, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configuration &gt; Templates &gt; Features &amp; Technologies.</td>
</tr>
<tr>
<td>2</td>
<td>In the Features and Technologies menu on the left, expand the My Templates folder and choose the template that you want to update.</td>
</tr>
<tr>
<td>3</td>
<td>Click the Tag icon, enter a tag name in the Tag as text box, then click Save.</td>
</tr>
</tbody>
</table>

Related Topics
- My Tags
Controller Templates

This section describes how to add and apply wireless templates. Templates allow you to set fields that you can then apply to multiple devices without having to reenter the common information.

The controller templates provide access to all Cisco Prime Infrastructure templates from a single page. You can add and apply controller templates, view templates, or make modifications to the existing templates. This section also includes steps for applying and deleting controller templates and creating or changing access point templates.

To access the controller templates, choose Configuration > Templates > Features & Technologies > Features and Technologies > Controller.

Related Topics
- Controller Templates and Field Descriptions
- Creating Controller Templates
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
- Configuring Client Profiling
- Configuring Mobile Concierge (802.11u)
- Access Point Groups

Associating a Tag With Multiple Templates

You can tag a new tag name or associate an existing tag with multiple templates.

Step 1
Choose Configuration > Templates > Features & Technologies.

Step 2
Click the Tag icon on the navigation toolbar of the Templates column.

Step 3
Enter a tag name in the Tag as field.

Step 4
In the My Templates folder, click the templates that are to be associated with the tag.
To associate all of the templates in the folder with the tag, select the check box next to the My Templates folder.

Step 5
Click Apply.

Related Topics
- My Tags
- Tagging an Existing Template
- Tagging a New Configuration Template
Creating Controller Templates

To create Features and Templates, follow these steps:

**Step 1** Choose **Configuration > Templates > Features & Technologies > Features and Technologies > Controller > Controller template.**

**Step 2** Hover your mouse cursor over the tool tip next to the template type and click **New** to create the template.

**Step 3** Complete the required fields.

If you are creating a feature template that applies only to a particular device type, the Device Type field lists only the applicable device type, and you cannot change the selection. Specifying a device type helps you to prevent a mismatch; that is, you cannot create a configuration and apply the configuration to a wrong device.

**Step 4** Click the Ports radio button, if you want to apply the template to a set of selected interfaces across selected devices.

The template will be tagged as port based template.

**Step 5** Click **Save as New Template**. After you save the template, apply it to your devices.

**Step 6** To verify the status of a template deployment, choose **Administration > Dashboard > Jobs Dashboard**.

To modify the deployment parameters for any subsequent configuration template deployments, select a configuration job, then click **Edit Schedule**.

**Related Topics**

- Controller Templates and Field Descriptions

Adding Controller Templates

To add a new controller template:

**Step 1** Choose **Configuration > Features & Technologies > Controller.**

**Step 2** Select the template you want to add.

**Step 3** Enter the template name.

Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

**Step 4** Provide a description of the template.

**Step 5** Click **Save**.
Deleting Controller Templates

To delete a controller template:

**Step 1** Choose Configuration > Features & Technologies > My Templates.
**Step 2** Select the template(s) you want to delete, then click Delete.
**Step 3** Click OK to confirm the deletion. If this template is applied to controllers, the Remove Template Confirmation page opens and lists all controllers to which this template is currently applied.
**Step 4** Select the check box of each controller from which you want to remove the template.
**Step 5** Click OK to confirm the deletion or Cancel to close this page without deleting the template.

Related Topics
- Adding Controller Templates
- Applying Controller Templates

Applying Controller Templates

You can apply a controller template directly to a controller or to controllers in a selected configuration group.

To apply a controller template, follow these steps:

**Step 1** Choose Configuration > Features & Technologies > Controller.
**Step 2** From the left sidebar menu, choose the category of templates to apply.
**Step 3** Click the template name for the template that you want to apply to the controller.
**Step 4** Click Apply to Controllers to open the Apply to Controllers page.
**Step 5** Select the check box for each controller to which you want to apply the template.
To select all controllers, select the check box that appears at the left most corner of the controllers table.
Select the Ignore errors on Apply template to Controllers check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.
**Step 6** Choose between applying the template directly to a controller or to all controllers in a selected configuration group.
To apply the template directly to a controller (or controllers), follow these steps:

a. Select the Apply to controllers selected directly radio button. The Apply to Controllers page lists the IP address for each available controller along with the controller name and the configuration group name (if applicable).
b. Select the check box for each controller to which you want to apply the template.
Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

To apply the template to all controllers in a selected configuration group, follow these steps:

a. Select the **Apply to controllers in the selected Config Groups** radio button. The Apply to Controllers page lists the name of each configuration group along with the mobility group name and the number of controllers included.

b. Select the check box for each configuration group to which you want to apply the template.

Configuration groups which have no controllers cannot be selected to apply the templates.

**Step 7** You can perform the following additional operations:

- If you select the Save Config to Flash after apply check box, the save config to Flash command is executed after the template is applied successfully.
- If you select the Reboot Controller after apply check box, the controller reboots after the template is successfully applied.

This configuration results can be viewed in the Template Results page by enabling the View Save Config / Reboot Results option.

**Step 8** Click **Save**.

You can apply some templates directly from the Template List page. Select the check box(es) of the template(s) that you want to apply, choose **Apply Templates** from the Select a command drop-down list, and click **Go** to open the Apply to Controllers page. Select the check box(es) of the controllers to which you want to apply this template, and click **OK**.

**Related Topics**

- Adding Controller Templates
- Applying Controller Templates

**Configuring Client Profiling**

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form.

Follow these guidelines when configuring client profiling:

By default, client profiling will be disabled on all WLANs.

- Client profiling is supported on access points that are in Local mode and FlexConnect mode.
- Profiling is not supported for clients in the following scenarios:
  - Clients associating with FlexConnect mode APs in Standalone mode.
  - Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.
Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.

The type of DHCP server used does not affect client profiling.

If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.

The client is identified based on the MAC address sent in the Accounting request packet.

Only MAC address should be sent as calling station ID in accounting packets when profiling is enabled.

With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.

To configure client profiling, follow these steps:

**Step 1** Choose **Configuration > Templates > Features & Technologies > Controller > WLANs > WLAN Configuration**.

**Step 2** Click the **Advanced** tab.

**Step 3** Select the **DHCP Profiling** check box to enable DHCP profiling.

**Step 4** Select the **HTTP Profiling** check box to enable HTTP profiling.

HTTP client profiling is supported since controller Version 7.3.1.31.

**Step 5** Click **Save**.

**Related Topics**
- Controller > WLANs > WLAN Configuration > Advanced

### Configuring Mobile Concierge (802.11u)

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

To configure Mobile Concierge (802.11u) groups:

**Step 1** Choose **Configuration > Templates > Features & Technologies > Controller > WLANs > WLAN Configuration**.

**Step 2** Click the **Hot Spot** tab.
Access Point Groups

Step 3 Complete the required fields on the following tabs:

- 802.11u Configuration
- Others
- Realm
- Service Advertisements
- Hotspot 2.0

Step 4 Click Save as New Template.

Related Topics
- Controller > WLANs > WLAN Configuration

Access Point Groups

- AP Groups (for controllers Release 5.2 and later) are referred to as AP Group VLANs for controllers prior to 5.2.
- To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.
- Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.
- The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

Related Topics
- Creating WLAN AP Groups Templates
- Adding Access Point Groups
- Deleting Access Point Groups

Creating WLAN AP Groups Templates

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits include more effective management of load balancing and bandwidth allocation.

To configure WLAN AP Groups, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > WLANs > AP Groups.

The WLAN > AP Groups page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.
Step 2

If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP Groups template page appears.

This page displays a summary of the AP groups configured on your network. In this page, you can add, remove, edit, or view details of an AP group. Click in the Edit column to edit its access point(s). Select the check box in the WLAN Profile Name column, and click **Remove** to delete WLAN profiles.

The maximum characters that you can enter in the Description text box is 256.

---

**Adding Access Point Groups**

You can create or modify a template for dividing the WLAN profiles into AP groups.

**Step 1**

Choose **Configuration > Templates > Features & Technologies > Controller > WLANs > AP Groups**.

**Step 2**

Choose **Add Template** from the Select a command drop-down list, and click **Go**.

**Step 3**

Enter a name and group description for the access point group. The group description is optional.

**Step 4**

If you want to add a WLAN profile, click the **WLAN Profiles** tab and configure the following fields:

a. Click **Add**.

b. Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

c. Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

   To display all available interfaces, delete the current interface from the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

d. Select the **NAC Override** check box, if applicable. The NAC override feature is disabled by default.

e. Specify the policy configuration parameters by clicking the **Add/Edit** link.

   - Policy Name—Name of the policy.
   - Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority. Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

f. When access points and WLAN profiles are added, click **Save**.

**Step 5**

If you want to add a RF profile, click the **RF Profiles** tab, and configure the following fields:

- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
• 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
• When RF profiles are added, click **Save**.

**Step 6**
To add a venue group, click the Venue Group tab, and configure the following fields:
• Select a venue group from the Venue Group drop-down list.
• Venue a venue type from the Venue Type drop-down list.
• Select the operator class(es) check box.
• Under the Multiple Venue List, click Add Row to create multiple venue list and configure the following:
  – Enter the language name that is used at the venue. Venue language should be 2 or 3 characters.
  – Enter the venue name that is associated with the basic service set (BSS).
  – Click **Save**.

**Step 7**
To configure Hyperlocation config parameters, click the Location Settings tab, and configure the following fields:
• Hyperlocation—By enabling this option, all the APs associated to that controller which have the Hyperlocation module will be enabled.
• Packet Detection RSSI Minimum—Adjust this value to filter out weak RSSI readings from location calculation.
• Scan Count Threshold for Idle Client Detection—The maximum permissible count of the idle clients detected while scanning.
• NTP Server IP Address—Enter the valid NTP server IP address. This IP address is used by all APs for time synchronization.
• Click **Save**.

**Step 8**
To map the Remote LAN to the ports, click the Ports tab, and do the following. Cisco 1810W Series Access Point comes with three LAN ports. The first LAN port contains a POE through which you can configure the POE status. You must add all the Remote LANs while creating AP groups in the WLAN Profiles tab.

Mapping the Remote LAN to the port is a two step process.
• You must first add the mapping and save the template. See **Step 4**.
• Map the Remote LAN. To do this:
  – From the Remote LAN Name drop-down list, choose the Remote LAN name.
  – Select the Port Status check box and POE Status check box.

**Note**
If the Remote LAN is disabled, you cannot map remote LAN to the AP group.

• Click **Save**.

**Related Topics**
• Access Point Groups
• Controller > 802.11 > RF Profiles
Deleting Access Point Groups

To delete an access point group, follow these steps:

Step 1  Choose Configuration > Templates > Features & Technologies.
Step 2  Choose Controller > WLANs > AP Groups from the left sidebar menu.
Step 3  Click Remove.

Related Topics
- Access Point Groups
- Creating WLAN AP Groups Templates
- Adding Access Point Groups

Creating Policy Configuration Templates

The Policy Configuration Templates page enables you to configure the device-based policies on the controller. You can configure policies for a user or a device on the network. The maximum number of policies that you can configure is 64. Policies are not applied on WLANs and AP groups if AAA override is configured on the controller.

To configure Policy Configuration templates:

Step 1  Choose Configuration > Templates > Features & Technologies > Controller > WLANs > Policy Configuration.
Step 2  If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go.
Step 3  Configure the required fields.
Step 4  Click Save as New Template.

Adding FlexConnect Users to FlexConnect AP Groups Templates

You can click the Users configured in the group link that appears when the FlexConnect Local Authentication check box is enabled to view the list of FlexConnect users. You can create FlexConnect users only after you save the FlexConnect AP Group. Maximum 100 FlexConnect users are supported in controller Release 5.2.x.x and later. If controller Release 5.2.0.0, and earlier supports only 20 FlexConnect users.

To delete a FlexConnect User, choose a user from the FlexConnect Users list, and then click Delete.

To configure a FlexConnect user, follow these steps:

Step 1  Choose Configuration > Features & Technologies > Controller > FlexConnect > FlexConnect AP Groups.
Step 2  Hover the mouse on **FlexConnect AP Groups** and select **Show All Templates**.

Step 3  Click the **Local Authentication** tab and select the **FlexConnect Local Authentication** check box to enable local authentication for this FlexConnect group.

Step 4  Click the **Users configured in the group** link. The FlexConnect Users page appears.

Step 5  If you want to add a new user, choose **Add User** from the Select a command drop-down list, and click **Go**. The **Add User** page appears.

Step 6  In the **User Name** text box, enter the FlexConnect username.

Step 7  In the **Password** text box, enter the password.

Step 8  Reenter the password in the **Confirm Password** text box.

Step 9  Click **Save**.

**Related Topics**
- Controller > FlexConnect > FlexConnect AP Groups

## Creating General AAA Security Controller Templates

To add a new template with general security information for a controller, follow these steps:

Step 1  Choose **Configuration > Templates > Features & Technologies > Controller > Security**.

Step 2  Choose **AAA > General - AAA** from the left sidebar menu.

Step 3  Click **New** beside the template you want to add.

Step 4  Configure the following fields:
- **Template Name**—Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.
- **Maximum Local Database Entries (on next reboot)**—Enter the maximum number of allowed database entries. This becomes effective on the next reboot.
- **Mgmt User Re-auth Interval**—Enter the termination interval for management users.

Step 5  Click **Save**.

Step 6  The template appears in the Template List page. In the Template List page, you can apply this template to controllers.

**Related Topics**
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
RADIUS Authentication Templates

You can add a RADIUS authentication template or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

Related Topics
- Controller > Security > AAA > RADIUS Auth Servers

Creating RADIUS Fallback Templates

To add and configure a RADIUS Fallback template or modify an existing template, follow these steps:

Step 1
Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > RADIUS Fallback.

Step 2
From the RADIUS Fallback Mode drop-down list, choose one of the following:
- Off—Disables fallback.
- Passive—You must enter a time interval.
- Active—You must enter a username and time interval.

Step 3
Click Save.

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates

Creating RADIUS TACACS Fallback Templates

To add and configure a RADIUS TACACS Fallback template or modify an existing template, follow these steps:

Step 1
Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > RADIUS TACACS+ Fallback.

Step 2
From the Radius Fallback group box, configure the following:
- From the Radius Fallback Mode drop-down list, you can choose one of the following:
  – Off—Disables fallback.
  – Passive—You must enter a time interval.
  – Active—You must enter a username and time interval.

Step 3
From the TACACS Fallback group box, configure the following:
- Choose either Enable or Disable from the Fallback Mode drop-down list.
- In the Time Interval text box, enter a value for TACACS Fallback test interval in seconds.
Step 4  Click Save as New Template.

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates

Local EAP General Templates

This page allows you to specify a timeout value for local EAP. You can then add or make changes to an existing local EAP general template.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

Related Topics
- Creating Network User Priority Templates

Creating Network User Priority Templates

You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add or make modifications to an existing network user credential retrieval priority template.

Step 1  Choose Configuration > Templates > Features & Technologies > Controller > Security > Local EAP > Network Users Priority.

Step 2  Use the left and right arrow keys to include or exclude network user credentials in the right page.

Step 3  Use the up and down keys to determine the order credentials are tried.

Step 4  Click Save.

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
Local Network Users Templates

With this template, you can store the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP might use the local user database as its back end database to retrieve user credentials. This page allows you to add or make modifications to an existing local network user template. You must create a local net user and define a password when logging in as a web authentication client.

Related Topics
- Creating Local Network Users Templates

Creating Local Network Users Templates

To configure a Local Network Users template, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Configuration &gt; Templates &gt; Features &amp; Technologies &gt; Controller &gt; Security &gt; AAA &gt; Local Net Users.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click Import CSV to import from a file, then click Browse to navigate to the file. Then continue to Step 6. If you disable the import, continue to Step 3. Only CSV file formats are supported. Prime Infrastructure reads data from the second row onwards. The first row in the file is treated as the header and the data is not read by Prime Infrastructure. The header can either be blank or filled.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter the following details:</td>
</tr>
<tr>
<td></td>
<td>• Username</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• Profile</td>
</tr>
<tr>
<td></td>
<td>• Description. The Profile column if left blank (or filled in with any profile) means a client on any profile can use this account.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Use the drop-down list to choose the SSID which this local user is applied to or choose the any SSID option.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enter a user-defined description of this interface.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
- Local Network Users Templates
User Login Policies Templates

You can set the maximum number of concurrent logins that each single user can have.

To add a user login template or make modifications to an existing template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > User Login Policies.
Step 2 Enter the maximum number of concurrent logins each single user can have.
Step 3 Click Save as New Template.

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
- User Login Policies Templates

MAC Filter Template

To add a MAC filter template or make modifications to an existing template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > MAC Filtering or choose Security > MAC Filtering.
Step 2 Click Import CSV to import a file containing access point MAC addresses.
Step 3 Enter the desired file path or click Browse to import the file.
   The import file must be a CSV file with MAC address, profile name, interface, and description (such as 00:11:22:33:44:55, Profile1, management, test filter). If you disable the Import from File check box, continue to Step 4.
   The client MAC address appears.
Step 4 Choose the profile name to which this MAC filter is applied or choose the Any Profile option.
Step 5 Use the drop-down list to choose from the available interface names.
Step 6 Enter a user-defined description of this interface.
Step 7 Click Save as New Template.
   You cannot use MAC address in the broadcast range.

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
Access Point or MSE Authorization Templates

These templates are devised for Cisco 11xx/12xx series access points converted from Cisco IOS to lightweight access points or for 1030 access points connecting in bridge mode. See the Cisco Mobility Services Engine Configuration Guide for further information.

To add a MSE authorization template or make modifications to an existing template, follow these steps:

Step 1  Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > AP or MSE Authorization.

Step 2  Click Import CSV to import a file containing access point MAC addresses.

You can only import a CSV file. The file format parallels the fields in the GUI and therefore includes access point base radio MAC, Type, Certificate Type (MIC or SSC), and key hash (such as 00:00:00:00:00:00, AP, SSC, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx). No other file formats are not supported.

Step 3  Enter the desired file path or click Browse to import the file.

Step 4  Click Save As New Template.

You cannot use MAC address in the broadcast range.

Related Topics

- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
- Access Point or MSE Authorization Templates

Manually Disabled Client Template

This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

Step 1  Choose Configuration > Templates > Features & Technologies > Controller > Security > Manually Disable Clients.

Step 2  Enter the MAC address of the client you want to disable.

Step 3  Enter a description of the client you are setting to disabled.

Step 4  Click Save as New Template.

You cannot use a MAC address in the broadcast range.

Related Topics

- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
Client Exclusion Policies Templates

To add a client exclusion policies template or modify an existing client exclusion policies template, follow these steps:

**Step 1** Choose **Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > Client Exclusion Policies**.

**Step 2** Complete the following fields:

- **Template Name**—Enter a name for the client exclusion policy.
- **Excessive 802.11 Association Failures**—Enable to exclude clients with excessive 802.11 association failures.
- **Excessive 802.11 Authentication Failures**—Enable to exclude clients with excessive 802.11 authentication failures.
- **Excessive 802.1X Authentication Failures**—Enable to exclude clients with excessive 802.1X authentication failures.
- **Excessive 802.11 Web Authentication Failures**—Enable to exclude clients with excessive 802.11 web authentication failures.
- **IP Theft or Reuse**—Enable to exclude clients exhibiting IP theft or reuse symptoms.

**Step 3** Click **Save as New Template**

**Related Topics**

- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates

Access Point Authentication and MFP Templates

Management Frame Protection (MFP) provides for the authentication of 802.11 management frames by the wireless network infrastructure. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy. An access point must be a member of a WDS to transmit MFP frames.

When MFP detection is enabled, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system.

To add or make modifications for the access point authentication and management frame protection (MFP) template, follow these steps:
**Chapter 26      Using Templates to Configure Devices**

**Access Point Groups**

---

**Step 1**  Choose Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > AP Authentication and MFP.

**Step 2**  From the Protection Type drop-down list, choose one of the following authentication policies:

- **None** — No access point authentication policy.
- **AP Authentication** — Apply authentication policy.
- **MFP** — Apply management frame protection.

Alarm trigger threshold appears only when AP authentication is selected as a protection type. Set the number of hits from an alien access point to ignore before raising an alarm. The valid range is from 1 to 255. The default value is 255.

**Step 3**  Click Save as New Template.

---

**Related Topics**

- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
- Access Point Authentication and MFP Templates

---

**Web Authentication Templates**

With web authentication, guests are automatically redirected to a web authentication page when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts might be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. You can use this template to replace the Web authentication page provided on the controller.

To add or make modifications to an existing web authentication template, follow these steps:

**Step 1**  Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > Web Auth Configuration.

**Step 2**  Choose one of the following web authentication type from the drop-down list.

- **default internal** — You can still alter the page title, message, and redirect URL, as well as whether the logo appears. Continue to Step 5.
- **customized web authentication** — Click Save and apply this template to the controller. You are prompted to download the web authentication bundle.

Before you can choose customized web authentication, you must first download the bundle by going to Config > Controller and choose Download Customized Web Authentication from the Select a command drop-down list, and click Go.

- **external** — you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.
Step 3 Select the **Logo Display** check box if you want your company logo displayed.

Step 4 Enter the title you want displayed on the Web Authentication page.

Step 5 Enter the message you want displayed on the Web Authentication page.

Step 6 Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user would be directed to the company home page.

Step 7 Click **Save as New Template**.

**Related Topics**
- Customized Web Authentication Page

**Customized Web Authentication Page**

You can download a customized Web Authentication page to the controller. With a customized web page, you can establish a username and password for user web access.

When downloading customized web authentication, you must follow these strict guidelines:
- Provide a username.
- Provide a password.
- Retain a redirect URL as a hidden input item after extracting from the original URL.
- Extract the action URL and set aside from the original URL.
- Include scripts to decode the return status code.

**Related Topics**
- Downloading Customized Web Authentication Pages

**Downloading Customized Web Authentication Pages**

Before downloading, follow these steps:

**Step 1** Download the sample login.html bundle file from the server. The following figure displays .html file. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.
Step 2 Edit the login.html file and save it as a .tar or .zip file. You can change the text of the Submit button to read Accept terms and conditions and Submit.

Step 3 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add IP address of TFTP server).

- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.

- A third-party TFTP server cannot run on the same computer as Prime Infrastructure because the built-in TFTP server of Prime Infrastructure and third-party TFTP server use the same communication port.

Step 4 Download the .tar or .zip file to the controller(s). The controller allows you to download up to 1 MB of a .tar file containing the pages and image files required for the Web authentication display. The 1 MB limit includes the total size of uncompressed files in the bundle. You can now continue with the download.

Step 5 Copy the file to the default directory on your TFTP server.

Step 6 Choose Configuration > Network > Network Devices > Wireless Controller.

Step 7 Click on a Device Name. If you select more than one device, the customized Web authentication page is downloaded to multiple controllers.

Step 8 From the left sidebar menu, choose System > Commands.

Step 9 From the Upload/Download Commands drop-down list, choose Download Customized Web Auth, and click Go.

Step 10 The IP address of the controller to receive the bundle and the current status are displayed.

Step 11 Choose local machine from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also select TFTP server.

For a local machine download, either .zip or .tar file options exists, but Prime Infrastructure does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files would be specified.
Step 12 Enter the maximum number of times the controller should attempt to download the file in the Maximum Retries field.

Step 13 Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout field.

Step 14 The files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click Browse to navigate to it.

Step 15 Click OK.

If the transfer times out, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of Prime Infrastructure. Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of Prime Infrastructure server, and the download web page now automatically populates the filename.

Step 16 Click the Click here to download a sample tar file link to get an option to open or save the login.tar file.

Step 17 After completing the download, you are directed to the new page and able to authenticate.

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates
- Web Authentication Templates

External Web Auth Server Templates

To create or modify an External Web Auth Server template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > External Web Auth Server or choose Security > External Web Auth Server.

Step 2 Enter the server address of the external web auth server.

Step 3 Click Save as New Template.

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates

Security Password Policy Template

To add or make modifications to an existing password policy template, follow these steps:
Step 1  Choose **Configuration > Templates > Features & Technologies > Controller > Security > Password Policy**.

Step 2  You can enable or disable the following settings:
- Password must contain characters from at least 3 different classes such as uppercase letters, lowercase letters, digits, and special characters.
- No character can be repeated more than 3 times consecutively.
- Password cannot be the default words like cisco or admin.
  Password cannot be “cisco”, “ocsic”, “admin”, “nimda’ or any variant obtained by changing the capitalization of letters, or by substituting ‘1” “i” or “!” for i, or substituting “0” for “o”, or substituting “$” for “s”.
- Password cannot contain username or reverse of username.

Step 3  Click **Save**.

**Related Topics**
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates

### Security - Access Control Templates

This section contains the following topics:
- Creating an Access Control List Template
- Creating a FlexConnect Access Control List Template
- Controller > Security > IP Groups
- Controller > Security > Protocol Groups

**Creating an Access Control List Template**

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs can be applied to data traffic to and from wireless clients or to all traffic destined for the controller Central Processing Unit (CPU) and can now support reusable grouped IP addresses and reusable protocols. After ACLs are configured in the template, they can be applied to the management interface, the AP-manager interface, or any of the dynamic interfaces for client data traffic; to the Network Processing Unit (NPU) interface for traffic to the controller CPU; or to a WAN.

You can create or modify an ACL template by protocol, direction, and the source or destination of the traffic.

You can now create new mappings from the defined IP address groups and protocol groups. You can also automatically generate rules from the rule mappings you created. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add up to 29 rules.

Existing ACL templates are duplicated into a new ACL template. This duplication clones all the ACL rules and mappings defined in the source ACL template.
This release of Prime Infrastructure provides support to IPv6 ACLs.

Related Topics
- Adding or Modifying an ACL Template
- Controller > Security > IP Groups
- Controller > Security > Protocol Groups

Adding or Modifying an ACL Template

To add or modify an existing ACL template, follow these steps:

**Step 1**
Choose Configuration > Templates > Features & Technologies > Controller > Security > Access Control Lists.

**Step 2**
Complete the following fields:
- Access Control List Name—User-defined name of the template.
- ACL Type—Choose either IPv4 or IPv6. IPv6 ACL is supported from controller Release 7.2.x.

**Step 3**
Choose IP Groups from the left sidebar menu to create reusable grouped IP addresses and protocols.

**Step 4**
Choose Add IP Group from the Select a command drop-down list and click Go to define a new IP address group.

One IP address group can have a maximum of 128 IP address and netmask combinations. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens. For the IP address of any, an any group is predefined.

**Step 5**
Edit the following current IP group fields if required in the ACL IP Groups details page:
- IP Group Name
- IP Address
- Netmask OR CIDR Notation
  Enter the Netmask or CIDR Notation and then click Add. The list of IP addresses or Netmasks appears in the List of IP Address/Netmasks text box.

  CIDR or Classless InterDomain Routing a protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks. CIDR notation allows you to add a large number of clients that exist in a subnet range by configuring a single client object.

  Netmask allows you to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property.
- BroadCast/Network
- List of IP Addresses/Netmasks
  Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or Netmask.

**Step 6**
Choose Access Control > Protocol Groups from the left sidebar menu to define an additional protocol that is not a standard predefined one.

The protocol groups with their source and destination port and DSCP are displayed.

**Step 7**
Choose Add Protocol Group from the Select a command drop-down list, and click Go to create a new protocol group. To view or modify an existing protocol group, click the URL of the group.
The Protocol Groups page appears.

**Step 8** Enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the parameters of a rule, the action for this rule is exercised.

**Step 9** Choose one of the following protocols from the drop-down list:
- Any—All protocols
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol
- ICMP—Internet Control Message Protocol
- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP—Internet Protocol
- Eth Over IP—Ethernet over Internet Protocol
- Other Port OSPF—Open Shortest Path First
- Other—Any other IANA protocol (http://www.iana.org/)

Some protocol choices (such as TCP or UDP) cause additional Source Port and Dest Port GUI elements to appear.
- Source Port—Specify the source of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.
- Dest Port—Specify the destination of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

**Step 10** Choose any or specific from the DSCP (Differentiated Services Code Point) drop-down list. If you choose specific, enter the DSCP (range of 0 to 255).

DSCP is a packet header code that can be used to define the quality of service across the Internet.

**Step 11** Click **Save**.

**Step 12** Choose the ACL template to which you want to map the new groups to define a new mapping. All ACL mappings appear on the top of the page, and all ACL rules appear on the bottom.

**Step 13** Choose Add Rule Mappings from the Select a command drop-down list. The Add Rule Mapping page appears.

**Step 14** Configure the following fields:
- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Direction—Any, Inbound (from client) or Outbound (to client).
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

**Step 15** Click **Add**. The new mappings populate the bottom table.

**Step 16** Click **Save**.
Chapter 26      Using Templates to Configure Devices

Access Point Groups

Step 17 Choose the mappings for which you want to generate rules, and click Generate. This automatically creates the rules.

Related Topics
- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates

Creating a FlexConnect Access Control List Template

You can create or modify a FlexConnect ACL template for configuring the type of traffic that is allowed by protocol, and the source or destination of the traffic. The FlexConnect ACLs do not support IPv6 addresses.

Creating and Applying a FlexConnect Access Control List

To configure and apply an Access Control List template to a Controller, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > FlexConnect ACLs.
Step 2 Enter a name for the new FlexConnect ACL.
Step 3 Click Save as New Template.
   A FlexConnect ACL template is created. You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All FlexConnect ACL mappings appear on the top of the page, and all FlexConnect ACL rules appear in the bottom.
Step 4 Click Add Rule Mappings, then configure the following fields in the FlexConnect ACL IP Protocol Map page:
   - Source IP Group—Predefined groups for IPv4 and IPv6.
   - Destination IP Group—Predefined groups for IPv4 and IPv6.
   - Protocol Group—Protocol group to use for the ACL.
   - Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.
Step 5 Click Add. The new mappings populate the bottom table.
Step 6 Click Save.
Step 7 Choose the mappings for which you want to generate rules, and click Generate. This automatically creates the rules.
Step 8 From the Select a command drop-down list in the FlexConnect ACL page, choose Apply Templates.
The Apply to Controllers page appears.
Step 9 Select Save Config to Flash after apply check box to save the configuration to Flash after applying the FlexConnect ACL to the controller.
Step 10 Select Reboot Controller after apply to reboot the controller once the FlexConnect ACL is applied. This check box is available only when you select the Save Config to Flash after apply check box.
## Creating Security - CPU Access Control List Templates

CPU ACL configuration with IPv6 is not supported in this release because all IP addresses of controllers on interfaces use IPv4 except the virtual interface. The existing ACLs are used to set traffic controls between the Central Processing Unit (CPU) and Network Processing Unit (NPU).

### Creating a CPU Access Control List (ACL) Template

To add or modify an existing CPU ACL template, follow these steps:

2. Select the check box to enable CPU ACL. When CPU ACL is enabled and applied on the controller, Prime Infrastructure displays the details of the CPU ACL against that controller.
3. From the ACL Name drop-down list, choose a name from the list of defined names.
Step 4  From the **CPU ACL Mode** drop-down list, choose which data traffic direction this CPU ACL list controls. The choices are the wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.

Step 5  Click **Save as New Template**.

---

**Creating Security - Rogue Templates**

Rogue templates enable you to configure the rogue policy (for access points and clients) applied to the controller. It also determines whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

Rogue access point rules allow you to define rules to automatically classify rogue access points. Prime Infrastructure applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time). Rogue access point rules also help reduce false alarms.

The new enhancements to the role classification rule are applicable for Cisco WLC 7.4 and later. These enhancements are not applicable to Catalyst 3850, Catalyst 3650, Catalyst 4500 switches, and Cisco 5760 WLAN Controllers (WLC).

To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > Rogue AP Rules**.

Rogue classes include the following types:

- **Malicious Rogue**—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
- **Friendly Rogue**—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
- **Unclassified Rogue**—A detected access point that does not match the malicious or friendly rules.

**Related Topics**

- Controller > Security > Wireless Protection Policies > Rogue Policies
- Controller > Security > Wireless Protection Policies > Rogue AP Rules
- Controller > Security > Wireless Protection Policies > Ignored Rogue AP
Creating a Rogue AP Rule Groups Template

A rogue access point rule group template allows you to combine more than one rogue access point rule to controllers. To view current rogue access point rule group templates or create a new rule group, follow these steps:

2. Enter a template name.
3. To add a Rogue AP rule, click to highlight the rule in the left column. Click Add to move the rule to the right column.
   - Rogue access point rules can be added from the Rogue Access Point Rules section.
4. To remove a rogue access point rule, click to highlight the rule in the right column. Click Remove to move the rule to the left column.
5. Use the Move Up/Move Down buttons to specify the order in which the rules apply. Highlight the desired rule and click Move Up or Move Down to move it higher or lower in the current list.
6. Click Save to confirm the rogue access point rule list.
7. Click Deploy to confirm the rogue access point rule list.

Related Topics
- Controller > Security > Wireless Protection Policies > Rogue AP Rules
- Deploying a Rogue AP Rule Groups Template
- Viewing Deployed Rogue AP Rules

Deploying a Rogue AP Rule Groups Template

After you create and save a rogue AP Rule Group template, you can deploy it to a controller.
Creating Security - Rogue Templates

Chapter 26      Using Templates to Configure Devices

Creating Security - Rogue Templates

Step 1 Navigate to the Rogue AP Rule Group that you previously created. By default, it is saved in Configuration > Templates > Features & Technologies > My Templates > Features & Technologies > Controller > Security > Wireless Protection Policies.

Step 2 Click Deploy to apply the rule group to the controller.

Step 3 Select the controller(s) to which you want to apply the AP Rule Group, then click OK. Prime Infrastructure creates a job for deploying the rules to the controllers you specified.

Step 4 Choose Administration > Dashboards > Job Dashboard > User Jobs > Config Deploy - Deploy View to view the status of the job.

Related Topics
- Controller > Security > Wireless Protection Policies > Rogue AP Rules
- Creating a Rogue AP Rule Groups Template
- Viewing Deployed Rogue AP Rules

Viewing Deployed Rogue AP Rules

You can view and edit the Rogue AP Rules that you previously deployed.

Step 1 Choose Monitor > Network > Network Devices > Wireless Controllers.

Step 2 Click on a Device Name, then select Security > Wireless Protection Policies > Rogue AP Rules.

Step 3 Click on a Rogue AP Rule name to edit the rule.

Step 4 To view Rogue AP alarms, click the Alarm Summary at the top right of the page, then select Rogue AP. You can also choose Dashboard > Wireless > Security to view Rogue AP information.

SIP Snooping

Keep the following guidelines in mind when using SIP Snooping:
- SIPs are available only on the Cisco 5500 Series Controllers and on the 1240, 1130, and 11n access points.
- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

Creating SIP Snooping

To configure SIP Snooping for a controller, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > 802.11 > SIP Snooping.
Step 2 Configure the following fields:

- **Port Start**
- **Port End**

If single port is to be used, configure both start and end port fields with same number.

Step 3 Click **Save as New Template**.

### Related Topics
- SIP Snooping
- Controller > 802.11 > Load Balancing
- Controller > 802.11 > Band Select
- Controller > 802.11 > Preferred Call
- Controller > 802.11 RF Profiles

### Creating Management Templates

You can create or modify the templates for the following management parameters of the controllers.

- Trap Receivers
- Trap Control
- Telnet and SSH
- Multiple Syslog servers
- Local Management Users
- Authentication Priority

### Related Topics
- Controller > Management > Trap Control
- Creating Telnet SSH Templates
- Controller > Management > Local Management User
- Creating User Authentication Priority Templates

### Creating Telnet SSH Templates

To add or modify a Telnet SSH configuration template, follow these steps:

Step 1 Choose **Configuration > Features & Technologies > Controller > Management > Telnet SSH**.

Step 2 Hover the mouse on **Telnet SSH** and select **Show All Templates**. The Management > Telnet SSH page appears, and to modify an existing template, click the template name. The number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the session timeout, maximum sessions, and whether Telnet or SSH sessions are allowed. The last column indicates when the template was last saved.
Chapter 26 Using Templates to Configure Devices

Creating Security - Rogue Templates

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, hover the mouse on Telnet SSH and select New or click Telnet SSH. The Telnet SSH template page appears.

Step 4 In the Session Timeout field, enter the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. The valid range is 0 to 160, and the default is 5.

Step 5 In the Maximum Sessions field, enter the number of simultaneous Telnet sessions allowed. The valid range is 0 to 5, and the default is 5. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port.

Step 6 Use the Allow New Telnet Session drop-down list to determine if you want new Telnet sessions allowed on the DS port. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the service port. The default is no.

Step 7 Use the Allow New SSH Session drop-down list to determine if you want Secure Shell Telnet sessions allowed. The default is yes.

Step 8 Click Save as New Template.

Related Topics

- Controller > Management > Trap Control
- Controller > Management > Local Management User
- Creating User Authentication Priority Templates

Creating Multiple Syslog Templates

You can enter up to three syslog server templates. To add or modify a multiple syslog configuration template, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller > Management > Multiple Syslog.

Step 2 Hover the mouse on Multiple Syslog and select Show All Templates. The Management > Multiple Syslog page appears, and to modify an existing template, click the template name. The number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the syslog server address. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 3 If you want to add a new template, hover the mouse on Multiple Syslog and select New or click Multiple Syslog. The Multiple Syslog template page appears.

Step 4 In the Syslog Server IP Address field, enter the appropriate syslog server IP address.

Step 5 Click Save as New Template.
Creating User Authentication Priority Templates

Management user authentication priority templates control the order in which authentication servers are used to authenticate the management users of a controller.

To add a user authentication priority template or make modifications to an existing template, follow these steps:

---

**Step 1** Choose Configuration > Features & Technologies > Controller > Management > Authentication Priority.

**Step 2** Hover the mouse on Authentication Priority and select Show All Templates. The Management > Authentication Priority page appears, and to modify an existing template, click the template name. The number of controllers and virtual domains that the template is applied to automatically populates. This initial page also displays the authentication priority list. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

**Step 3** If you want to add a new template, hover the mouse on Authentication Priority and select New or click Authentication Priority. The Local Management Users template page appears.

**Step 4** Select either First or Second radio buttons to prioritize the authentication of the local server.

**Step 5** Select either RADIUS or TACACS+ radio buttons to try if local authentication fails.

**Step 6** Click Save as New Template.

---

Related Topics

- Controller > Management > Trap Control
- Creating Telnet SSH Templates
- Controller > Management > Local Management User

Creating LyncSDN Templates

LyncSDN configuration is not supported on Virtual and Cisco 2500 Series and Virtual Controllers.

You can create these LyncSDN templates:

- LyncSDN Global Config feature templates.
- LyncSDN PolicyFeature templates.
- LyncSDN ProfileFeature templates
Creating LyncSDN Global Configuration Template

To create parameters to apply to devices using the LyncSDN Global Config feature, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Features &amp; Technologies &gt; Controller &gt; LyncSDN &gt; LyncSDN Global Config.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Ports radio button, if you want to apply the template to a set of selected interfaces across selected devices. The template will be tagged as port based template.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Template Detail area, configure the following information:</td>
</tr>
<tr>
<td></td>
<td>• Select the LyncServer checkbox to enable or disable the LYNC application on the Prime Infrastructure.</td>
</tr>
<tr>
<td></td>
<td>• Enter the port number.</td>
</tr>
<tr>
<td></td>
<td>You can configure support for HTTP/HTTPS communication on Prime Infrastructure for LYNC server. Prime Infrastructure supports only http. For https certificate, you need to provide and approved at Lync server which takes once Lync service is ready from Prime Infrastructure.</td>
</tr>
<tr>
<td>Step 6</td>
<td>When you are finished, click Save as Template.</td>
</tr>
</tbody>
</table>

Creating LyncSDN Policy Template

To create parameters to apply to devices using the LyncSDN Policy feature, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Features &amp; Technologies &gt; Controller &gt; LyncSDN &gt; LyncSDN Policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Ports radio button, if you want to apply the template to a set of selected interfaces across selected devices. The template will be tagged as port based template.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Template Detail area, configure the following information:</td>
</tr>
</tbody>
</table>
• Choose the policy of audio lync call on WLAN from the Audio drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.

• Choose the policy of video lync call on WLAN from the Video drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.

• Choose the policy of desktop-share lync call on WLAN from the Application-Sharing drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.

• Choose the policy of file transfer lync call on WLAN from the File-Transfer drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.

Step 6 When you are finished, click **Save as Template**.

---

**Related Topics**

- Creating LyncSDN Global Configuration Template
- Creating LyncSDN Profile Template

---

**Creating LyncSDN Profile Template**

To create parameters to apply to devices using the LyncSDN Profile feature, follow these steps:

- **Step 1** Choose **Configuration > Features & Technologies > Controller > LyncSDN > LyncSDN Policy**.

- **Step 2** In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

- **Step 3** Click the Ports radio button, if you want to apply the template to a set of selected interfaces across selected devices.

  The template will be tagged as port based template.

- **Step 4** In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

- **Step 5** In the Template Detail area, click the Wlan Profile check box and select a policy from the LyncSDN Policy drop-down list.

- **Step 6** When you are finished, click **Save as Template**.

---

**Related Topics**

- Creating LyncSDN Global Configuration Template
- Creating LyncSDN Policy Template

---

**Creating AVC Profiles Templates**

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1400 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.
AVC is supported only on the following controllers:
- Cisco 2500 and 5500 Series Controllers.
- WiSM 2 Controllers
- Cisco Flex 7500 and Cisco 8500 Series Controllers.

To configure the AVC profile template, follow these steps:

Step 1: Choose Configuration > Features & Technologies > Controller > Application Visibility And Control > AVC Profiles.

Step 2: If you want to add a new template, hover the mouse on AVC Profiles and select New or click AVC Profiles. To modify an existing template, click the template name.

Step 3: In the AVC Profile Name text box, enter the AVC Profile Name.

Note: You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application. This allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs.

Step 4: Under the AVC Rule List, click Add Row to create AVC rules.
- In the Application Name field, enter the name of the application.
- In the Application Group Name field, enter the name of the application group to which the application belongs.
- From the Action drop-down list, choose one of the following:
  - Drop—Drops the upstream and downstream packets corresponding to the chosen application.
  - Mark—Marks the upstream and downstream packets corresponding to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
  - Rate Limit—If you select Rate Limit as an action, you can specify Average Rate Limit per client and Burst rate limit. The number of rate limit applications is limited to 3.
  
  The default action is to permit all applications.

- If you select Mark as an action, then choose QoS levels from the DSCP drop-down list. DSCP is a Packet header code that is used to define quality of service across the Internet. The DSCP values are mapped to the following QoS levels:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)—Provides lowest bandwidth for guest services.
  - Custom—Specify the DSCP value. The range is from 0 to 63.

- In the DSCP Value field, enter the value which can be entered only when Custom is chosen from the DSCP drop-down list.

- If you select Rate Limit as an action, you can specify the value in Avg. Rate Limit (in Kbps), which is the average bandwidth limit of that application.
If you select Rate Limit as an action, you can specify Burst Rate Limit (in Kbps), which is the peak limit of that application.

**Step 5**

Click **Save as New Template**.

---

**Related Topics**

- Adding Controller Templates
- Deleting Controller Templates
- Applying Controller Templates

## Creating NetFlow Templates

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing. This protocol collects IP traffic information from network devices to monitor traffic. The NetFlow architecture consists of the following components:

- **Collector**—An entity that collects all the IP traffic information from various network elements.
- **Exporter**—A network entity that exports the template with the IP traffic information. The controller acts as an exporter.

**Related Topics**

- Creating NetFlow Monitor Template
- Creating NetFlow Exporter Template

## Creating NetFlow Monitor Template

To create NetFlow Monitor template:

**Step 1**

Choose **Configuration > Templates > Features & Technologies > Controller > Netflow > Monitor**.

**Step 2**

Hover your mouse cursor over the tool tip next to the template type and click **New** to create.

**Step 3**

Complete the required fields, then and click **Save as New Template**.

---

**Related Topics**

- Creating NetFlow Templates

## Creating NetFlow Exporter Template

You can configure only one NetFlow Exporter per controller. To create NetFlow exporter template:

**Step 1**

Choose **Configuration > Templates > Features & Technologies > Controller > Netflow > Monitor**.

**Step 2**

Hover your mouse cursor over the tool tip next to the template type and click **New** to create.
Step 3  Complete the required fields, then and click **Save as New Template**.

---

**Related Topics**
- Creating NetFlow Templates

---

**Configuring EoGRE Tunneling**

Ethernet over GRE (EoGRE) is the new aggregation solution for aggregating Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. When the IP GRE tunnels are terminated on a service provider broadband network gateway, the end host’s traffic is terminated and subscriber sessions are initiated for the end host.

---

**Step 1**  Choose **Configuration > Templates > Features & Technologies > Features and Technologies > Controller > Tunneling > Configuration**.

**Step 2**  To create tunnel gateways:
- Set the **Heartbeat Interval**. The default interval is 60 seconds.
- Set **Max Heartbeat Skip Count**. The default value is set to 3.
  - If the TGW does not reply after three keepalive pings, the Cisco WLC marks the TGW as nonoperational. The number of skip count decides how many times the TGW can skip consecutive replies, before the Cisco WLC knows that the TGW is nonoperational.
- Under **Tunnel Gateway**, click **Add Row** and configure the tunnel gateway:
  - Specify a Tunnel Gateway name.
  - Specify the Tunnel Gateway IP address. Both IPv4 and IPv6 address formats are supported. You can create up to 10 such tunnel gateways.
  - Click **Save**.
- In the **Domain**, click **Add Row** and configure the domain. Domain is the grouping of two tunnel gateways.
  - Specify a domain name.
  - From the **Tunnel Gateway** drop-down list, choose the tunnel gateway.
  - Click **Save**.

**Step 3**  Provide a name for the template and click **Save as New Template**.

**Step 4**  To create a tunnel profile:
- Choose **Tunneling > EoGRE Profile**, and select the **Basic** radio button.
- Specify the **TGW1 IP** address.
- Specify the **TGW2 IP** address.
- Specify the **VLAN Id**.
- To select a WLAN, use the **Quick Filter** and enter the **WLAN** name in the text box, or check the check boxes of the applicable WLANs, and click **Save as New Template**.

**Step 5**  To define a tunnel profile rule:
• Choose **Tunneling > EoGRE Profile**, and select the **Advanced** radio button.

• Under the **Rule** tab, configure the following:
  – Click the tunnel profile that you created.
  – Under the Rule tab, to map a specific realm to the profile, enter the realm name. A realm is a string after @, for example, user_name@realm. To match any Realm, use *, which means all realms are accepted.
  – Choose Tunnel Type as EoGRE.
  – Set the **VLAN**.
  – Choose the **Gateway Domain** that you created in Step 2.
  – Click **Save**.

**Step 6** Configure Tunnel Parameters under the **Tunnel Parameters** tab:

• Check the **Gateway as AAA Proxy** and **Gateway as Accounting Proxy** (optional) check boxes to configure a tunnel gateway as a AAA proxy and as an Accounting proxy.

• (Optional) Check the **DHCP Option-82** check box.

• Choose the **DHCP Option 82** format as either **Binary** or **ASCII**.

• Specify the **DHCP Option 82 Delimiter**. The default is ;.

• Specify the **Circuit-ID** and **Remote-ID** information. You can choose up to five fields each and sort them accordingly.

**Step 7** Click **Save as New Template**.

**Step 8** To associate the tunnel profile to the WLAN:

• Choose **Configuration > Features & Technologies > Features and Technologies > Controller > WLANs > WLAN Configuration > Advanced** tab.

• Under Tunneling, choose the **Tunnel Profile**.

---

**Related Topics**

• Adding Controller Templates

• Deleting Controller Templates

• Applying Controller Templates

---

**Creating AP Configuration Templates**

This menu provides access to the access point templates summary details. Use the selector group box to access and configure the respective templates details.

• **Configuring a New Lightweight Access Point Template**

• **Creating Autonomous Access Point Templates**

---

**Configuring a New Lightweight Access Point Template**

To configure a new Lightweight Access Point template, follow these steps:
Creating AP Configuration Templates

Step 1 Choose **Configuration > Templates > Lightweight Access Points**.

Step 2 Choose **Add Template** from the Select a command drop-down list and click **Go**.

Step 3 Enter a template name in the text box.

Step 4 Enter a template description in the text box.

Step 5 Click **Save as New Template**.

The Lightweight AP Template Detail page contains the following tabs:

- AP Parameters
- Mesh
- 802.11a/n/ac
- 802.11a SubBand
- 802.11b/g/n
- 802.11a/b/g/n
- CDP
- FlexConnect

**Related Topics**

- Selecting Access Point Source for AP Template Deployment
- Selecting Access Points for Template Deployment
- Scheduling Template Deployment

**Selecting Access Point Source for AP Template Deployment**

Based on the AP Source selection, the appropriate visualization is loaded on the AP Selection tab.

To select the AP Source:

Step 1 Choose **Configuration > Templates > Lightweight Access Points**.

Step 2 Click the applicable Template Name link in the Lightweight Access Point page.

Step 3 Click the **AP Source** tab and select the visualization:

- **Select APs Manually**—If you select this option, you must select APs manually while trying to push the LWAP template configuration to the APs.
- **Site Maps**—If you select this option, you can select dynamic location based Site Maps for deployment of LWAP template configuration.

**Related Topics**

- Selecting Access Points for Template Deployment
- Scheduling Template Deployment
Selecting Access Points for Template Deployment

You can deploy the template using the AP Selection or Schedule tabs.
To deploy access point template:

**Step 1** Choose Configuration > Templates > Lightweight Access Points.
**Step 2** Click the applicable Template Name link in the Lightweight Access Points page.
**Step 3** Click the AP Selection tab and select one or more access points by selecting their respective check boxes. You can use the Filter feature to search for specific access points. Here the visualization is loaded based on the AP Source selection.
**Step 4** Click Deploy to save and deploy the template to the relevant access points.
**Step 5** Click Apply to save and apply the AP/Radio parameters to the selected access points from the search.

Related Topics
- Scheduling Template Deployment

Scheduling Template Deployment

**Step 1** Choose Configuration > Templates > Lightweight Access Points.
**Step 2** Click the applicable Template Name link in the Lightweight Access Points page.
**Step 3** Click the Schedule tab.
This allows you to save the current template, apply the current template immediately, or schedule the current template to start the provisioning at the applicable time.
- Start Time—Allows you to configure and start the template deployment at a scheduled time.
  - Now—Deploys the template right away.
  - Date—Enter a date in the text box or use the calendar icon to select a start date.
- Recurrence—Select from none, hourly, daily, or weekly to determine how often this scheduling occurs.

Related Topics
- Configuring a New Lightweight Access Point Template

Viewing the Status of the Template Deployment

You can deploy a maximum of 6000 templates to APs.

**Step 1** Choose Configuration > Templates > Lightweight Access Points.
**Step 2** Click the applicable Template Name link in the Lightweight Access Points page.
**Step 3**  Click the **Deploy Status** tab and displays all recently applied reports including the apply status and the date and time the apply was initiated. Click the link that is available on the number of access points (next to the Template Deployed to APs field) to view the deployment status information.

- Graph shows the Success or Partial Success status. Click the graph to view status information.
- The Deploy Status section shows the following information:
  - AP Name
  - Status—Indicates success, partial failure, failure, or not initiated. For failed or partially failed provisioning, click **Details** to view the failure details (including what failed and why it failed).
  - Ethernet MAC—Indicates the Ethernet MAC address for the applicable access point.
  - Controller IP—Indicates the controller IP address for the applicable access point.
  - AP IP
  - Controller Name
  - AP Model
  - Campus
  - Building
  - Floor
  - Outdoor Area
  - FlexConnect Group

**Related Topics**
- Configuring a New Lightweight Access Point Template

**Editing a Lightweight Access Point Template**

To edit an existing Lightweight Access Point Template, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Lightweight Access Points.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the applicable template in the Template Name column.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Make any necessary changes to the current lightweight access point template or schedule.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Configuring a New Lightweight Access Point Template

**Creating Autonomous Access Point Templates**

The Configuration > Templates > Autonomous Access Point templates page allows you to configure CLI templates for autonomous access points.

- Configuring a New Autonomous Access Point Template, page 26-lix
- Wireless Configuration Templates, page 26-lxxvii
Creating AP Configuration Templates

Configuring a New Autonomous Access Point Template

To configure a new Autonomous Access Point template, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Templates &gt; Autonomous Access Points.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the Select a command drop-down list, choose Add Template.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Go.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a Template Name.</td>
</tr>
</tbody>
</table>
| Step 5 | Enter the applicable CLI commands.  
Do not include any show commands in the CLI commands text box. The show commands are not supported. |
| Step 6 | Click Save. |

Related Topics

* Creating Autonomous Access Point Templates

Applying an AP Configuration Template to an Autonomous Access Point

To apply an AP Configuration template to an autonomous access point, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Configuration &gt; Templates &gt; Autonomous Access Points.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the template name link to select a template and apply it to the an autonomous access point. The New Autonomous AP Configuration template page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter a Template Name.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the applicable CLI commands.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Apply to Autonomous Access Points. The Apply to Autonomous Access Points page appears.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Select the desired autonomous access point.</td>
</tr>
</tbody>
</table>
| Step 8 | Click OK.  
Select the Ignore errors on Apply template to Controllers check box to ignore errors and apply all commands in the template to the Autonomous AP. If this check box is not selected, any errors encountered while applying a command in the template to a Autonomous AP causes the rest of the commands to be not applied. |

Related Topics

* Creating Autonomous Access Point Templates
Viewing Template Results

To view the results when you apply an Autonomous AP Configuration template to an access point, follow these steps:

Step 1 Choose **Configuration > Templates > Autonomous AP**.
Step 2 Click the template name link to select a template and apply it to the autonomous access point. The Autonomous AP Configuration template page appears.
Step 3 Enter a **Template Name**.
Step 4 Enter the applicable CLI commands.
Step 5 Click **Save**.
Step 6 Click **Apply to Autonomous Access Points**. The Apply to Autonomous Access Points page appears.
Step 7 Select the desired autonomous access point.
Step 8 Click **OK**. The Template Results page appears. The following parameters appear:

- **IP Address** — IP address of the access point.
- **AP Name** — The name of the access point.
- **Apply Status** — Indicates success, failure, initiated or not initiated.
- **Operation Status** — Displays the operational status: Success or Failure.
- **Reason** — Indicates the reasons for failure.
- **Session Output**

Related Topics
- Creating Autonomous Access Point Templates

Configuring Switch Location Configuration Templates

You can configure the location template for a switch using the Switch Location Configuration template. To configure a location template for a switch, follow these steps:

Step 1 Choose **Configuration > Templates > Switch Location**.
The Switch Location Configuration template page appears.
Step 2 From the Select a command drop-down list, choose **Add Template**, and click **Go**.
Step 3 Complete the required fields in the New Template page.

Related Topics
- Switch Location Configuration Template
Creating Autonomous AP Migration Templates

When you migrate an already-managed autonomous access point to lightweight, its location and antenna information is migrated as well. You do not need to reenter the information. Prime Infrastructure automatically removes the autonomous access point after migration.

The Migration Analysis option does not run during discovery by default. If you prefer to run the migration analysis during discovery, choose Administration > Settings > CLI Session to enable this option.

Prime Infrastructure also supports the migration of autonomous access point to CAPWAP access point. Choose Configuration > Templates > Autonomous AP Migration to access this page.

Related Topics
- Migrating an Autonomous Access Point to a Lightweight Access Point
- Viewing the Current Status of Cisco IOS Access Points

Migrating an Autonomous Access Point to a Lightweight Access Point

To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to lightweight access points. Choose Configuration > Autonomous AP Migration.

The Autonomous AP Migration Templates list page displays the following information:
- Name—The template name.
- Description—The description of template.
- AP Count—The number of autonomous access points selected for migration.
- Schedule Run—The time at which the task is scheduled to run.
- Status—Indicates one of the following task statuses:
  - Not initiated—The template is yet to start the migration and starts at the scheduled time.
  - Disabled—The template is disabled and does not run at the scheduled time. This is the default state for a template when it is created without selecting any autonomous access points.
  - Expired—The template did not run at the scheduled time (this might be due to Prime Infrastructure server being down).
  - Enabled—The template is yet to start the migration and starts at the scheduled time.
  - In progress—The template is currently converting the selected autonomous access points to CAPWAP.
  - Success—The template has completed the migration of autonomous access point to CAPWAP successfully.
  - Failure—The template failed to migrate all the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.
  - Partial Success—The template failed to migrate a subset of the selected autonomous access point to CAPWAP. You can check the detailed status about the failures by using the View Migration Status page.

Once an access point is converted to lightweight, the previous status or configuration of the access point is not retained.
From the Select a command drop-down list, the following functions can be performed:

- Add Template—Allows you to provide necessary information for migration.
- Delete Templates—Allows you to delete a current template.
- View Migration Report—Allows you to view information such as AP address, migration status (in progress or fail), timestamp, and a link to detailed logs.
- View Current Status— Allows you to view the progress of the current migration (updated every three seconds).
- View Migration Analysis Summary—Lists the pass or fail status as required for an access point conversion. Only those access points with all criteria as pass are eligible for conversion.

**Related Topics**
- Autonomous AP Migration Templates > Add Template
- Editing Current Autonomous AP Migration Templates

**Editing Current Autonomous AP Migration Templates**

To edit a current migration template, follow these steps:

**Step 1** Choose Configuration > Templates > Autonomous AP Migration.

**Step 2** Click the migration template in the Name column.

**Step 3** Edit the necessary parameters:

- General
  - Name—Indicates the user-defined name of the migration template.
  - Description—Enter a brief description to help you identify the migration template.

- Upgrade Options
  - DHCP Support—Click to enable Dynamic Host Configuration Protocol support. This ensures that after the conversion every access point gets an IP from the DHCP server.
  - Retain AP HostName—Click to enable retention of the same hostname for this access point. The hostname is retained in the CAPWAP, only when you are migrating the AP to CAPWAP for the first time. It might not be retained if you are upgrading an AP for several times. The CAPWAP access points hostname is set to default if autonomous access points hostname has more than 32 characters.
  - Migrate over WANLink—If you enable this option, the $env_vars file stores the remote TFTP server location. This information is copied to the AP. If this option is not selected, then Prime Infrastructure internal TFTP server is used to copy the $env_vars file to AP.
  - DNS Address—Enter the DNS address.
  - Domain Name—Enter the domain name.

- Controller Details
  Ensures that the access point authorization information (SSC) can be configured on this controller and the converted access points can join.
Creating Autonomous AP Migration Templates

- Controller IP
- AP Manager IP
- User Name
- Password

• TFTP Details
  - TFTP Server IP
  - File Path
  - File Name

• Schedule Details
  - Apply Template
  - Notification (Optional)

**Step 4**
Click **Save**.

**Related Topics**
- Creating Autonomous AP Migration Templates

**Viewing the Migration Analysis Summary**

To view the Migration Analysis Summary, follow these steps:

**Step 1**
Choose **Configuration > Templates > Autonomous AP Migration**.

**Step 2**
Choose **View Migration Analysis Summary** from the Select a command drop-down list, and click **Go**. The Migration Analysis Summary page appears.

The autonomous access points are eligible for migration only if all the criteria have a pass status. A red X designates ineligibility, and a green checkmark designates eligibility. These columns represent the following:

• Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.

• Software Version Criteria—Conversion is supported only in Cisco IOS Release 12.3(7)JA excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.

• Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only

• Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.
Related Topics

- Creating Autonomous AP Migration Templates

Adding/Modifying a Migration Template

If you want to add a migration template:

1. Choose Configuration > Templates > Autonomous AP Migration.
2. Choose Add Template from the Select a command drop-down list.
3. To modify an existing template, click the template name from the summary list.
4. Add or modify the required migration parameters.
5. Click Save.

Once a template is added in Prime Infrastructure, the following additional buttons appear:

- Select APs—Choosing this option provides a list of autonomous access points in Prime Infrastructure from which to choose the access points for conversion. Only those access points with migration eligibility as pass can be chosen for conversion.
- Select File—To provide CSV information for access points intended for conversion.

Related Topics

- Autonomous AP Migration Templates

Copying a Migration Template

To copy a migration template, follow these steps:

1. Choose Configuration > Templates > Autonomous AP Migration.
2. Select the check box of the template you want to copy, and then choose Copy Template from the Select a command drop-down list.
3. Click Go.
4. Enter the name for the new template to which you want to copy the current template.

Related Topics

- Autonomous AP Migration Templates

Deleting Migration Templates

To delete migration templates, follow these steps:

1. Choose Configuration > Templates > Autonomous AP Migration.
2. Select the check box(es) of the template(s) you want to delete, and then choose Delete Templates from the Select a command drop-down list.
Step 3  Click **Go**.
Step 4  Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.

Related Topics

- Autonomous AP Migration Templates

## Viewing the Current Status of Cisco IOS Access Points

To view the current status of Cisco IOS Access point:

**Step 1**  Choose **Configuration > Templates > Autonomous AP Migration**.

**Step 2**  Select **View Current Status** from the Select a command drop-down list in the Autonomous AP Migration Templates page to view the status of Cisco IOS access point migration.

The following information is displayed:

- **IP Address**—IP address of the access point.
- **Status**—Current status of the migration.
- **Progress**—Summary of the migration progress.

Related Topics

- Autonomous AP Migration Templates

## Disabling Access Points that are Ineligible

If an autonomous access point is labeled as ineligible for conversion, you can disable it.

Related Topics

- Autonomous AP Migration Templates

## Deploying Templates

After you create a configuration template, and click **Deploy**, you can specify various deployment options as shown in **Table 26-2**.
### Deploying Templates

**Deployment Flow for Model Based Configuration Templates**

**Note** This deployment flow is not applicable for Controller based templates.

**Step 1** After you create a configuration template, click **Deploy**. The Deployment wizard page opens.

**Step 2** Select the devices on which you want to deploy the template, then click **Next** to choose the input values.

**Step 3** Select the ports on which you want to deploy the template, then click Next to choose the input values.

This option appears only if you have tagged the template as ports based, while creating the template.

### Table 26-2 Template Deployment Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Selection</td>
<td>Displays the list of devices to which you want to apply the template.</td>
</tr>
<tr>
<td>Value Assignment</td>
<td>Allows you to specify a variable other than what was previously defined in the configuration template. Click a name, and the previously defined variables are displayed. To change any of the values, click the variable that you want to change, enter a new value, and click <strong>Apply</strong>. You can also update the variables for all selected devices. Click <strong>All Selected Devices</strong> and update variables to apply the changes on all selected devices at the same time. If you want to update variables for a particular device in the list that need not be applicable to other devices, then choose the device and update its variables. All of the other devices will continue to use the variables that were previously defined except for the device for which variables are updated.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Allows you to create a meaningful deployment job name, then specify whether to run the job now or in the future. You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.</td>
</tr>
<tr>
<td>Job Option</td>
<td>The following job options are available:</td>
</tr>
<tr>
<td></td>
<td>• Failure Policy—</td>
</tr>
<tr>
<td></td>
<td>Ignore failure and continue—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.</td>
</tr>
<tr>
<td></td>
<td>Stop on failure—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn’t undergo template deployment, “Not Attempted” message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.</td>
</tr>
<tr>
<td></td>
<td>• Copy Running Config to Startup—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.</td>
</tr>
<tr>
<td></td>
<td>• Archive Config after deploy—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.</td>
</tr>
<tr>
<td>Summary</td>
<td>Summarizes your deployment option selections.</td>
</tr>
</tbody>
</table>
Step 4  In the **Input Values** tab, you can toggle between **Form** and **CLI** view.

Step 5  After entering the necessary configuration values, click **Next** or click **CLI** to confirm the device and template configuration values.

Step 6  Schedule the deployment job using **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:
  
  **Failure Policy**
  
  - **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  
  - **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn’t undergo template deployment, “Not Attempted” message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
  
  - **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
  
  - **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 7  Click **Next** to view the job deployment summary.

Step 8  On the Deployment Summary tab, you will see the CLI view for each of the device.

Step 9  Click **Finish** to deploy the template.

Step 10  Click **Job Status** in the pop-up dialog box to launch the **Job Dashboard** to view the status of the job.

---

### Global Variables

The global user variables are variables which are accessible in all scripts. Each user variable must have a name that begins with `gv`. The name should begin with alphabets. Special characters allowed are dot appended with `gv`, hyphen and underscore.

You can create, delete or edit a global variable.

---

**Step 1** Choose **Configuration > Templates > Global Variable.**

**Step 2** From the Define Global Variable page, click **Add Row.**

**Step 3** Specify a name, description, type and display label.

**Step 4** Click **Save** to save the new variable.

The global variables created here can be applied while creating the CLI and Features and Technologies templates.

**Related Topics**

- Creating CLI Configuration Templates
Shared Policy Objects

Policy objects enable you to define logical collections of elements. They are reusable, named components that can be used by other objects and policies. They also eliminate the need to define a component each time that you define a policy.

Objects are defined globally. This means that the definition of an object is the same for every object and policy that references it. However, many object types (such as interface roles) can be overridden at the device level. This means that you can create an object that works for most of your devices, then customize the object to match the configuration of a particular device that has slightly different requirements.

To improve efficiency and accuracy in your configuration templates, you can create shared policy objects to include in your configuration templates. You create interface roles or network objects that you can add to your configuration templates.

Related Topics
- Creating Interface Roles
- Creating Network Objects
- Creating a Security Rule Parameter Map
- Creating a Security Service Group
- Creating a Security Zone

Creating Interface Roles

Interface roles allow you to define policies to specific interfaces on multiple devices without having to manually define the names of each interface. Interface roles can refer to any of the actual interfaces on the device, including physical interfaces, subinterfaces, and virtual interfaces such as loopback interfaces.

If you create an all-Ethernets interface role, you can define identical advanced settings for every Ethernet interface on the device with a single definition. You add this interface role to a configuration template, then deploy the template to the selected devices to configure the Ethernet interfaces.

Interface roles are especially useful when applying policies to new devices. As long as the devices that you are adding share the same interface naming scheme as existing devices, you can quickly deploy the necessary configuration template containing the interface role to the new devices.

For example, you can use interface roles to define the zones in a zone-based firewall configuration template. You might define an interface role with a naming pattern of DMZ*. When you include this interface role in a template, the configuration is applied to all interfaces whose name begins with “DMZ” on the selected devices. As a result, you can assign a policy that enables anti-spoof checking on all DMZ interfaces to all relevant device interfaces with a single action.

Step 1 Choose Configuration > Templates > Shared Policy Objects.
Step 2 In the Shared Policy Objects pane, choose Shared > Interface Role.
Step 3 From the Interface Role page, click Add Object.
Chapter 26      Using Templates to Configure Devices

Step 4  From the Add Interface Role page, create matching rules for the interface role.

When you define the zone-based template, for example, all of the interfaces on the device that match the specified rules will become members of the security zone represented by this interface role. You can match interfaces according to their name, description, type, and speed.

Step 5  Click OK to save the configurations.

Related Topics
  - Shared Policy Objects

Creating Network Objects

Network objects are logical collections of IP addresses or subnets that represent networks. Network objects make it easier to manage policies.

There are separate objects for IPv4 and IPv6 addresses; the IPv4 object is called “networks/hosts,” and the IPv6 object is called “network/hosts-IPv6.” Except for the address notation, these objects are functionally identical, and in many instances the name network/host applies to either type of object. Note that specific policies require the selection of one type of object over the other, depending on the type of address expected in the policy.

You can create shared policy objects to be used in the following configuration templates:
  - Zone-based firewall template
  - Application Visibility

Step 1  Choose Configuration > Templates > Shared Policy Objects > Shared > IPv4 Network Object.
Step 2  From the Network Object page, click Add Object and add a group of IP addresses or subnets.
Step 3  Click OK to save the configurations.

Related Topics
  - Shared Policy Objects

Creating a Security Rule Parameter Map

To create and use a set of parameter map objects in the firewall rules, do the following:

Step 1  Choose Configuration > Templates > Shared Policy Objects.
Step 2  In the Shared Policy Objects pane, choose Shared > Security Rule Parameter Map.
Step 3  From the Security Rule Parameter Map page, click Add Object.
Step 4  Specify a name and description for the parameter map that is being created.
Step 5  From the parameters list, select the parameters you want to apply and provide a value for each of them.
Step 6  To specify Device Level Override, choose Device Level Override > Add Device.
Step 7  Select the device you wish to add, and click OK.
Step 8 Click OK to save the configurations.

Related Topics

- Shared Policy Objects

Creating a Security Service Group

To create and use a set of parameter map objects in the firewall rules, do the following:

Step 1 Choose Configuration > Templates > Shared Policy Objects.
Step 2 In the Shared Policy Objects pane, choose Shared > Security Service.
Step 3 From the Security Service page, click Add Object.
Step 4 Specify a name and description for the service that is being created.
Step 5 Select the service data from the available list. If you select TCP or UDP, provide a list of port numbers or port ranges (separated by comma).
Step 6 To specify Device Level Override, choose Device Level Override > Add Device.
Step 7 Select the device you wish to add, and click OK.
Step 8 Click OK to save the configurations.

Related Topics

- Shared Policy Objects

Creating a Security Zone

Step 1 Choose Configuration > Templates > Shared Policy Objects.
Step 2 In the Shared Policy Objects pane, choose Shared > Security Zone.
Step 3 From the Security Zone page, click Add Object.
Step 4 Specify a name and description for the security zone that is being created.
Step 5 Specify a set of rules that defines the interfaces that must be attached to the zone.
Step 6 To specify Device Level Override, choose Device Level Override > Add Device.
Step 7 Select the device you wish to add, and click OK.
Step 8 Click OK to save the configurations.

Related Topics

- Shared Policy Objects
Configuration Groups

You might want to associate a set of configuration templates with specific devices. If you have devices that require the same configuration, you can create a configuration group that associates configuration templates with devices. Creating a configuration group allows you to quickly apply new templates without remembering to which devices the new templates should be deployed.

Composite templates allow you to group smaller templates together, but only configuration groups specify the relationship between the templates and the groups of devices to which those templates apply.

Before you create a configuration group, you should:

- Create configuration templates for the devices in your configuration group.
- Determine which devices should be included in the configuration group.

Related Topics

- Features and Technologies Templates
- Grouping Configuration Templates with Devices

Grouping Configuration Templates with Devices

**Step 1** Choose Configuration > Templates > Configuration Groups.

**Step 2** Complete the required fields. The device types displayed depend on what you select from the Device Type field.

**Step 3** Where needed, change a template’s order in the group by selecting it and clicking the up or down arrow.

**Step 4** Click Save as a New Configuration Group. The possible configuration groups are:

- Success—Indicates that a configuration group has been successfully created.
- Pending—One or more devices in the configuration group have changes that have not yet been deployed. For example, if you add a new device to the configuration group, the status of the new device is Pending. If you modify a configuration template to which the configuration group is associated, all devices in the configuration group have the status Pending.
- Scheduled—Indicates that a configuration group deployment is scheduled. When a configuration group is Scheduled, any devices in the group that are Pending or Failed are changed to Scheduled. If a device is Deployed, it remains Deployed and its status does not change to Scheduled.
- Failure—Deployment has failed for one or more devices in the configuration group.

Related Topics

- Features and Technologies Templates
- Configuration Groups
WLAN Controller Configuration Groups

By creating a configuration group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all of the controllers in a group. You can add, delete, or remove configuration groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected configuration groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected configuration groups.

**Note**
A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

By choosing Configuration > Templates > WLAN Controller Configuration Groups, you can view a summary of all configuration groups in the Prime Infrastructure database. Choose Add Configuration Groups from the Select a command drop-down list to display a table with the following columns:

- Group Name—Name of the configuration group.
- Templates—Number of templates applied to the configuration group.

**Related Topics**
- Creating Controller Configuration Groups

Creating Controller Configuration Groups

To create a configuration group, follow these steps:

**Step 1** Choose Configuration > Templates > WLAN Controller Configuration Groups.

**Step 2** From the Select a command drop-down list, choose Add Config Group, then click Go.

**Step 3** Enter the new configuration group name. It must be unique across all groups.

- If Enable Background Audit is selected, the network and controller audits occur for this configuration group.
- If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.

**Step 4** Other templates created in Prime Infrastructure can be assigned to a configuration group. The same WLAN template can be assigned to more than one configuration group. Choose from the following:

- Select and add later—Click to add a template at a later time.
- Copy templates from a controller—Click to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new configuration group. Only the templates are copied.

**Note** The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.
**Step 5**  Click *Save*. The Configuration Groups page appears.

After you create a configuration group, Prime Infrastructure allows you to choose and configure multiple controllers by choosing the template that you want to push to the group of controllers.

- **General**—Allows you to enable mobility group.
  
  To enable the Background Audit option, set template-based audit in Administration > System > Audit Settings.

- **Controllers**

- **Country/DCA**

- **Templates**—Allows you to select the configuration templates that you have already created.

- **Apply/Schedule**

- **Audit**

- **Reboot**

- **Report**—Allows you to view the most recent report for this group.

---

**Related Topics**

- WLAN Controller Configuration Groups
- Adding or Removing Controllers from Configuration Groups
- Configuring Multiple Country Codes
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
- Rebooting Configuration Groups
- Retrieving Configuration Group Reports

---

**Adding or Removing Controllers from Configuration Groups**

To add or remove controllers from a configuration group, follow these steps:

**Step 1**  Choose Configuration > Templates > WLAN Controller Configuration Groups.

**Step 2**  Click a group name in the Group Name column, then click the *Audit* tab.

The columns in the table display the IP address of the controller, the configuration group name the controller belongs to, and the mobility group name of the controller.

**Step 3**  Click to highlight the row of the controller that you want to add to the group, then click *Add*.

**Step 4**  To remove a controller from the group, highlight the controller in the Group Controllers area and click *Remove*.

**Step 5**  Click the *Apply/Schedule* tab, click *Apply* to add or remove the controllers to the configuration groups, then click *Save Selection*.

---

**Related Topics**

- WLAN Controller Configuration Groups
Configuring Multiple Country Codes

You can configure one or more countries on a controller. After countries are configured on a controller, the corresponding 802.11a/n DCA channels are available for selection. At least one DCA channel must be selected for the 802.11a/n network. When the country codes are changed, the DCA channels are automatically changed in coordination.

Note

802.11a/n and 802.11b/n networks for controllers and access points must be disabled before configuring a country on a controller. To disable 802.11a/n or 802.11b/n networks, choose Configure > Controllers, select the desired controller that you want to disable, choose 802.11a/n or 802.11b/g/n from the left sidebar menu, and then choose Parameters. The Network Status is the first check box.

To add multiple controllers that are defined in a configuration group and then set the DCA channels, follow these steps:

**Step 1** Choose Configuration > Templates > WLAN Controller Configuration Groups.

**Step 2** From the Select a command drop-down list, choose Add Config Groups, then click Go.

**Step 3** Create a configuration group by entering the group name and mobility group name.

**Step 4** Click Save, then click the Controllers tab.

**Step 5** Highlight the controllers that you want to add, and click Add. The controller is added to the Group Controllers page.

**Step 6** Click the Country/DCA tab. The Country/DCA page appears. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

**Step 7** Select the Update Country/DCA check box to display a list of countries from which to choose.

**Step 8** Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes page. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking Save Selection.

A minimum of 1 and a maximum of 20 countries can be configured for a controller.

Related Topics

- WLAN Controller Configuration Groups
- Adding or Removing Controllers from Configuration Groups
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
Applying or Scheduling Configuration Groups

The scheduling function allows you to schedule a start day and time for provisioning. To apply the mobility groups, mobility members, and templates to all of the controllers in a configuration group, follow these steps:

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.
Step 2 Click a group name in the Group Name column, then choose the Apply/Schedule tab.
Step 3 Click Apply to start the provisioning of mobility groups, mobility members, and templates to all of the controllers in the configuration group. After you apply, you can leave this page or log out of Prime Infrastructure. The process continues, and you can return later to this page to view a report.

**Note** Do not perform any other configuration group functions during the provisioning process.

A report is generated and appears in the Recent Apply Report page. It shows which mobility groups, mobility members, or templates were successfully applied to each of the controllers.

Step 4 Enter a starting date in the text box or use the calendar icon to choose a start date.
Step 5 Choose the starting time using the hours and minutes drop-down lists.
Step 6 Click Schedule to start the provisioning at the scheduled time.

Related Topics
- WLAN Controller Configuration Groups
- Adding or Removing Controllers from Configuration Groups
- Configuring Multiple Country Codes
- Auditing Configuration Groups
- Rebooting Configuration Groups
- Retrieving Configuration Group Reports

Auditing Configuration Groups

The Configuration Groups Audit page allows you to verify if the configuration complies of the controller with the group templates and mobility group. During the audit, you can leave this window or log out of Prime Infrastructure. The process continues, and you can return to this page later to view a report.

Do not perform any other configuration group functions during the audit verification.

To perform a configuration group audit, follow these steps:

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.
WLAN Controller Configuration Groups

Chapter 26 Using Templates to Configure Devices

Step 2  Click a group name in the Group Name column, then click the Audit tab.

Step 3  Click to highlight a controller on the Controllers tab, choose > (Add), and Save Selection.

Step 4  Click to highlight a template on the Templates tab, choose > (Add), and Save Selection.

Step 5  Click Audit to begin the auditing process.

A report is generated and the current configuration on each controller is compared with that in the configuration group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

This audit does not enforce Prime Infrastructure configuration to the device. It only identifies the discrepancies.

Step 6  Click Details to view the Controller Audit report details.

Step 7  Double-click a line item to open the Attribute Differences page. This page displays the attribute, its value in Prime Infrastructure, and its value in the controller.

Step 8  Click Retain Prime Infrastructure Value to push all attributes in the Attribute Differences page to the device.

Step 9  Click Close to return to the Controller Audit Report page.

Related Topics
- WLAN Controller Configuration Groups
- Adding or Removing Controllers from Configuration Groups
- Configuring Multiple Country Codes
- Applying or Scheduling Configuration Groups
- Rebooting Configuration Groups
- Retrieving Configuration Group Reports

Rebooting Configuration Groups

Step 1  Choose Configuration > Templates > WLAN Controller Configuration Groups.

Step 2  Click a group name in the Group Name column, then click the Reboot tab.

Step 3  Select the Cascade Reboot check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.

Step 4  Click Reboot to reboot all controllers in the configuration group at the same time. During the reboot, you can leave this page or log out of Prime Infrastructure. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report page shows when each controller was rebooted and what the controller status is after the reboot. If Prime Infrastructure is unable to reboot the controller, a failure is shown.

Related Topics
- WLAN Controller Configuration Groups
- Adding or Removing Controllers from Configuration Groups
Retrieving Configuration Group Reports

To display all recently applied reports under a specified group name, follow these steps:

**Step 1** Choose Configuration > Templates > WLAN Controller Configuration Groups.

**Step 2** Click a group name in the Group Name column, then click the Report tab. The Recent Apply Report page displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:

- **Apply Status**—Indicates success, partial success, failure, or not initiated.
- **Successful Templates**—Indicates the number of successful templates associated with the applicable IP address.
- **Failures**—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
- **Details**—Click Details to view the individual failures and associated error messages.

**Step 3** To view the scheduled task reports, click the click here link at the bottom of the page.

**Related Topics**
- WLAN Controller Configuration Groups
- Adding or Removing Controllers from Configuration Groups
- Configuring Multiple Country Codes
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
- Rebooting Configuration Groups

**Wireless Configuration Templates**

The following sections describe how to create wireless configuration templates for:

- Lightweight access points
- Autonomous access points
- Switches
- Converting autonomous access points to lightweight access points

**Related Topics**
- Creating Lightweight AP Configuration Templates
Creating Lightweight AP Configuration Templates

To create a template for a lightweight access point, follow these steps:

Step 1: Choose Configuration > Templates > Lightweight Access Points.
Step 2: From the Select a command drop-down list, choose Add Template, then click Go.
Step 3: Enter a name and description for the template and click Save. If you are updating an already existing template, click the applicable template in the Template Name column.
Step 4: Click each of the tabs and complete the required fields.

Related Topics
- Lightweight AP Configuration Templates Field Description

Creating Autonomous AP Configuration Templates

To create a template for an autonomous access point, follow these steps:

Step 1: Choose Configuration > Templates > Autonomous Access Points.
Step 2: From the Select a command drop-down list, choose Add Template, then click Go. If you are updating an already existing template, click the applicable template in the Template Name column.
Step 3: Enter a name for the template and the applicable CLI commands.

Note: Do not include any show commands in the CLI commands text box. The show commands are not supported.

Creating Autonomous AP Migration Templates

To make a transition from an autonomous solution to a unified architecture, autonomous access points must be converted to lightweight access points.

After an access point has been converted to lightweight, the previous status or configuration of the access point is not retained.

To create an autonomous AP migration template, follow these steps:

Step 1: Choose Configuration > Autonomous AP Migration.
Step 2  From the Select a command drop-down list, choose Add Template, then click Go. If you are updating an already existing template, click the applicable template in the Template Name column.

Step 3  Complete the required fields. For information about the field descriptions, see the Cisco Prime Infrastructure 3.1 Reference Guide.

Step 4  To view the migration analysis summary, choose Monitor > Tools > Autonomous AP Migration Analysis.

Related Topics
• Autonomous AP Migration Templates

Creating Switch Location Templates

To configure a location template for a switch, follow these steps:

Step 1  Choose Configuration > Templates > Switch Location.

Step 2  From the Select a command drop-down list, choose Add Template, then click Go.

Step 3  Enter the required fields. For information about the field descriptions, see the Cisco Prime Infrastructure 3.1 Reference Guide.

Related Topics
• Switch Location Configuration Templates

Creating Controller WLAN Configuration Policy Templates

Use the Policy Configuration Templates page to configure device-based policies on a controller. You can configure policies for a user or a device on the network.

The maximum number of policies that you can configure is 64. Policies are not applied on WLANs and AP groups if AAA override is configured on the controller.

Step 1  Choose Configuration > Templates > Features and Technologies.

Step 2  From the left sidebar menu, choose Features and Technologies > Controller > WLANs > Policy Configuration. The Policy Configuration Template page displays.

Step 3  Complete the following fields:
• Name—Name of the policy template
• Description—Description of the policy template.
• Tags—Search keywords applicable to this template.
• Device Type (validation criteria)—The device product family, series or type used to validate the template (CUWN, for Cisco Unified Wireless Network, is the default).
• Policy Name—Name of the policy.
• Policy Role—The user type or the user group the user belongs to. For example, student, employee.
Wireless Configuration Templates

Chapter 26 Using Templates to Configure Devices

- **EAP Type**—EAP authentication method used by the client. The available types are as follows:
  - LEAP
  - EAP-FAST
  - EAP-TLS
  - PEAP
- **Device Type**—Choose the device type to which this policy applies (e.g., Apple Laptop).
- **VLAN ID**—VLAN associated with the policy.
- **IPv4 ACL**—Choose an IPv4 ACL for the policy from the list
- **QoS**—Choose the policy’s Quality of Service level from the list. You can choose one of the follows:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)—Provides the lowest bandwidth for guest services.
- **Session Timeout**—Maximum amount of time, in seconds, before a client is forced to re-authenticate. The default value is 0 seconds.
- **Sleeping Client Timeout**—Maximum amount of time, in hours, before a guest client is forced to re-authenticate. The default value is 12 hours. The range is from 1 to 720 hours.

**Step 4** When you are finished, click **Save as new template**.
CHAPTER 27

Configuring Wireless Devices

This section describes how to configure wireless devices in Prime Infrastructure and contains the following sections:

- Configuring Controllers
- Configuring Controller WLANs
- Configuring FlexConnect on APs
- Configuring Controller Security Parameters
- Configuring Third-Party Controllers and Access Points
- Configuring Switches
- Enabling Traps and Syslogs on Switches for Wired Client Discovery
- Configuring Unified Access Points
- Configuring Controller Redundancy
- Configuring Cisco Adaptive wIPS Profiles
- Managing MSE High Availability Using Prime Infrastructure

Configuring Controllers

The following sections describe how to configure your controllers using Prime Infrastructure:

- Viewing All Controllers
- Wireless Controller Summary Information
- Controller-Specific Commands
- Auditing Controllers
- Updating Controller Credentials
- Updating Controller Credentials in Bulk
- Rebooting Controllers
- Downloading Software to Controllers
- Configuring IPaddr Upload Configuration/Logs from Controllers
- Downloading IDS Signatures to Controllers
- Downloading Customized WebAuthentication Bundles to Controllers

Text Part Number:
Viewing All Controllers

You can view a summary of all controllers in the Prime Infrastructure database.

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** To use the command buttons at the top of the page, select the check box next to one or more controllers.

**Step 3** To view specific information about a controller, click on a Device Name.

**Related Topics**
- Wireless Controller Summary Information
- Controller-Specific Commands

### Wireless Controller Summary Information

When you choose Configuration > Network > Network Devices, select Device Type > Wireless Controller, then select a check box next to one or more controllers, summary information appears:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Name of the controller. Click on a device name to view device details, configure the controller, apply templates, view and schedule configuration archives, and view and update the controller software image.</td>
</tr>
<tr>
<td>Reachability</td>
<td>Reachability status is updated based on the last execution information of the Device Status background task.</td>
</tr>
<tr>
<td>IP Address/DNS</td>
<td>Local network IP address of the controller management interface. Click the icon under the IP address to launch the controller web user interface in a new browser window.</td>
</tr>
</tbody>
</table>
Chapter 27  Configuring Wireless Devices

Configuring Controllers

Related Topics

- Controller-Specific Commands

Controller-Specific Commands

When you choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller and select the checkbox next to one or more devices, the following buttons appear at the top of the page:

- Delete—Allows you to delete a controller.
- Edit—Allows you to edit general parameters, SNMP parameters, Telnet/SSH parameters, HTTP parameters, and IPSec parameters.
- Sync—
- Groups & Sites—Allows you to add and remove controllers from location groups and sites.
- Reboot—Enables you to confirm the restart of your controller after saving configuration changes. You can select these reboot options:
  - Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
  - Reboot APs
  - Swap AP Image
- Download—Allows you to select the following options to download software to controllers.
  - Download Software—Choose from TFTP, FTP, SFTP to download software to the selected controller or all controllers in the selected groups after you have a configuration group established.
  - Download IDS Signatures

### Table 27-1 Wireless Controller Summary Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Based on the series, device types are grouped. For example:</td>
</tr>
<tr>
<td></td>
<td>• WLC2100—21xx Series Wireless LAN Controllers</td>
</tr>
<tr>
<td></td>
<td>• 2500—25xx Series Wireless LAN Controllers</td>
</tr>
<tr>
<td></td>
<td>• 4400—44xx Series Wireless LAN Controllers</td>
</tr>
<tr>
<td></td>
<td>• 5500—55xx Series Wireless LAN Controllers</td>
</tr>
<tr>
<td></td>
<td>• 7500—75xx Series Wireless LAN Controllers</td>
</tr>
<tr>
<td></td>
<td>• WiSM—WiSM (slot number, port number)</td>
</tr>
<tr>
<td></td>
<td>• WiSM2—WiSM2 (slot number, port number)</td>
</tr>
<tr>
<td>AP Discovery Status</td>
<td>Indicates whether the AP discovery has completed.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The operating system release.version.dot.maintenance number of the code currently running on the controller.</td>
</tr>
<tr>
<td>Mobility Group Name</td>
<td>Name of the mobility or WPS group.</td>
</tr>
</tbody>
</table>
– Download Customized Web Auth
– Download Vendor Device Certificate
– Download Vendor CA Certificate
– Bulk Update Controllers

• Configure
  – Save Config to Flash
  – Discover Templates from Controller
  – Templates Applied to Controller
  – Audit Now
  – Update Credentials

Related Topics
• Viewing All Controllers
• Wireless Controller Summary Information
• Auditing Controllers
• Updating Controller Credentials in Bulk
• Rebooting Controllers
• Downloading Software to Controllers

Auditing Controllers

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click Configure > Audit Now.
Step 4 Click OK in the pop-up dialog box to remove the template associations from configuration objects in the database as well as template associations for this controller from associated configuration groups (This is a template-based audit only).

Related Topics
• Controller Audit Reports
• Viewing Templates Applied to Controllers

Controller Audit Reports

After you perform an audit on a controller, the Audit Report displays the following information:

• Device Name
• Time of Audit
• Audit Status
• Applied and Config Group Template Discrepancies information including the following:
  – Template type (template name)
  – Template application method
  – Audit status (For example, mismatch, identical)
  – Template attribute
  – Value in Prime Infrastructure
  – Value in Controller

• Other Prime Infrastructure Discrepancies including the following:
  – Configuration type (name)
  – Audit Status (For example, mismatch, identical)
  – Attribute
  – Value in Prime Infrastructure
  – Value in Controller
  – Total enforcements for configuration groups with background audit enabled. If discrepancies are found during the audit in regards to the configuration groups enabled for background audit, and if the enforcement is enabled, this section lists the enforcements made during the controller audit. If the total enforcement count is greater than zero, this number appears as a link. Click the link to view a list of the enforcements made from Prime Infrastructure.

• Failed Enforcements for Configuration Groups with background audit enabled—If the failed enforcement count is greater than zero, this number appears as a link. Click the link to view a list of failure details (including the reason for the failure) returned by the device.

• Restore Prime Infrastructure Values to Controller or Refresh Configuration from Controller—If there are configuration differences found as a result of the audit, you can either click Restore Prime Infrastructure Values to controller or Refresh Config from controller to bring Prime Infrastructure configuration in sync with the controller.
  – Choose Restore Prime Infrastructure Values to Controller to push the discrepancies to the device.
  – Choose Refresh config from controller to pick up the device for this configuration from the device. Templates are not refreshed as a result of clicking Refresh Config from Controller.

Related Topic
• Auditing Controllers

**Updating Controller Credentials**

To update SNMP and Telnet credentials, you must do so on each controller. You cannot update SNMP/Telnet credential details for multiple controllers at the same time.

SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can be displayed only and not modified.

To update the SNMP/Telnet credentials, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

**Step 2** Select the check box(es) of the applicable controller(s).
Step 3  Click Configure > Update Credentials.
Step 4  Complete the required fields, then click OK.

Related Topic
- Updating Controller Credentials in Bulk

**Updating Controller Credentials in Bulk**

You can update multiple controllers credentials by importing a CSV file.
To update controller(s) information in bulk, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, select Wireless Controllers.
Step 2  Select the check box(es) of the applicable controller(s).
Step 3  Click Download > Bulk Update Controllers.
Step 4  Enter the CSV filename in the Select CSV File text box or click Browse to locate the desired file.
Step 5  Click Update and Sync.

Related Topic
- Updating Controller Credentials
- Rebooting Controllers
- Replacing Old Controller Models with New Models
- Modifying Controller Properties

**Rebooting Controllers**

You should save the current controller configuration prior to rebooting. To reboot a controller, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, select Wireless Controllers, then click Reboot > Reboot Controllers.
Step 2  Select the required Reboot Controller option:
  - Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
  - Reboot APs—Select the check box to enable a reboot of the access point after making any other updates.
  - Swap AP Image—Indicates whether or not to reboot controllers and APs by swapping AP images. This could be either Yes or No.
Step 3 Click OK.

Related Topic
- Updating Controller Credentials
- Replacing Old Controller Models with New Models
- Modifying Controller Properties

Downloading Software to Controllers

To download software to a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controllers.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Download and select one of the following options:
- Download Software TFTP
- Download Software FTP
- Download Software SFTP

Step 4 Complete the required fields.

Step 5 Select the download type. The pre-download option is displayed only when all selected controllers are using Release 7.0.x.x or later.
- Now—Executes the download software operation immediately. If you select this option, proceed with Step 7.
- Scheduled—Specify the scheduled download options.
  - Schedule download to controller—Select this check box to schedule download software to controller.
  - Pre-download software to APs—Select this check box to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots. To see Image Predownload status per AP, enable the task in the Administration > Dashboards > Job Dashboard > System Jobs > Wireless Poller > AP Image Pre-Download Status, and run an AP Image Predownload report from the Report Launch Pad.
  - FlexConnect AP Upgrade—Select this option to enable one access point of each model in the local network to download the image. The remaining access points will then download the image from the master access point using the pre-image download feature over the local network, which reduces the WAN latency.

Step 6 Select the Schedule options.
Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download. If any AP is in pre-download progress state at the time of the scheduled reboot, the controller will not reboot. You must wait for the pre-download to finish for all the APs, and then reboot the controller manually.

Step 7 Enter the FTP credentials including username, password, and port.
You can use special characters such as @, #, ^, *, ~, -, +, =, {, ], :, ., and / in the password. You cannot use special characters such as $, ', \, %, &, (, ), ;, ", <, >, , , ? , and | as part of the FTP password. The special character "!" (exclamation mark) works when the password policy is disabled.

**Step 8**
Select whether the file is located on the **Local machine** or an **FTP Server**. If you select FTP Server, the software files are uploaded to the FTP directory specified during the installation.

**Step 9**
Click **Download**.

If the transfer times out, choose the FTP server option in the **File is located on** field; the server filename is populated and Prime Infrastructure retries the operation.

---

**Configuring IPaddr Upload Configuration/Logs from Controllers**

You can upload a controller system configuration to the specified TFP or TFTP server as a file. Both File FTP and TFTP are supported for uploading and downloading files to and from Prime Infrastructure. To upload files from a controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

**Step 2** Click a Device Name, then click the **Configuration** tab.

**Step 3** From the left sidebar menu, choose **System > Commands**.

**Step 4** Select the **FTP** or **TFTP** radio button, then select **Upload File from Controller** and click **Go**.

**Step 5** Complete the required fields.

Prime Infrastructure uses an integral TFTP and FTP server. This means that third-party TFTP and FTP servers cannot run on the same workstation as Prime Infrastructure because Prime Infrastructure and the third-party servers use the same communication port.

**Step 6** Click **OK**. The selected file is uploaded to your TFTP or FTP server and named what you entered in the **File Name** text box.

---

**Downloading IDS Signatures to Controllers**

Prime Infrastructure can download Intrusion Detection System (IDS) signature files to a controller. If you specify to download the IDS signature file from a local machine, Prime Infrastructure initiates a two-step operation:

1. The local file is copied from the administrator workstation to Prime Infrastructure’s built-in TFTP server.
2. The controller retrieves that file.

If the IDS signature file is already in the Prime Infrastructure server’s TFTP directory, the downloaded web page automatically populates the filename.

**Step 1** Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

**Step 2** Select the check box(es) of the applicable controller(s).

**Step 3** Click **Download > Download IDS Signatures**.
Step 4 Complete the required fields.

Step 5 Click Download.

If the transfer times out, choose the FTP server option in the File is located on field; the server filename is populated and Prime Infrastructure retries the operation.

Related Topics
- Viewing All Controllers
- Rebooting Controllers
- Downloading Software to Controllers
- Replacing Old Controller Models with New Models
- Modifying Controller Properties

**Downloading Customized WebAuthentication Bundles to Controllers**

You can compress the page and image files used for displaying a web authentication login page, known as webauth bundles, and download the file to a controller.

Controllers accept a .tar or .zip file of up to 1 MB in size. The 1 MB limit includes the total size of uncompressed files in the bundle.

To download customized web authentication bundles to a controller, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

**Step 2** Select the check box(es) of the applicable controller(s).

**Step 3** Click Download > Download Customized WebAuth.

**Step 4** To download an example login.tar bundle file, click on the preview image displayed, then edit the login.html file and save it as a .tar or .zip file. The file contains the pages and image files required for the web authentication display.

**Step 5** Download the .tar or .zip file to the controller.

**Step 6** Select where the file is located.

If you select local machine, you can upload either a .zip or .tar file type. Prime Infrastructure converts .zip files to .tar files. If you choose a TFTP server download, you can specify a .tar files only.

**Step 7** Complete the required fields, then click Download.

If the transfer times out, choose the FTP server option in the File is located on field; the server filename is populated and Prime Infrastructure retries the operation.

After Prime Infrastructure completes the download, you are directed to a new page and are able to authenticate.

Related Topics
- Viewing All Controllers
- Downloading Software to Controllers


- Replacing Old Controller Models with New Models
- Modifying Controller Properties

**Downloading Vendor Device Certificates to Controllers**

Each wireless device (controller, access point, and client) has its own device certificate. If you want to use your own vendor-specific device certificate, you must download it to the controller.

To download a vendor device certificate to a controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

**Step 2** Select the check box(es) of the applicable controller(s).

**Step 3** Click **Download > Download Vendor Device Certificate**.

**Step 4** Complete the required fields, then click **Download**.

**Related Topic**
- Downloading Vendor CA Certificates to Controllers
- Downloading Software to Controllers
- Replacing Old Controller Models with New Models
- Modifying Controller Properties

**Downloading Vendor CA Certificates to Controllers**

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate might be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, you must download it to the controller.

To download a vendor CA certificate to the controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

**Step 2** Select the check box(es) of the applicable controller(s).

**Step 3** Click **Download > Download Vendor Device Certificate**.

**Step 4** Complete the required fields, then click **Download**.

**Related Topic**
- Downloading Vendor Device Certificates to Controllers
- Viewing All Controllers
- Rebooting Controllers
- Downloading Software to Controllers
• Replacing Old Controller Models with New Models
• Modifying Controller Properties

Saving Controller Configurations to Flash

To save the configuration to flash memory, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click Configure > Save Config to Flash.

Related Topic
• Synchronizing Configurations from Controllers
• Rebooting Controllers
• Downloading Software to Controllers
• Replacing Old Controller Models with New Models
• Modifying Controller Properties

Synchronizing Configurations from Controllers

To synchronize the configuration from the controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click Sync, and Yes to proceed

Related Topic
• Saving Controller Configurations to Flash
• Rebooting Controllers
• Downloading Software to Controllers
• Replacing Old Controller Models with New Models
• Modifying Controller Properties

Managing Controller Templates

You can specify for which Prime Infrastructure configurations you want to have associated templates. The templates that are discovered do not retrieve management or local user passwords. The following rules apply for template discovery:
• Template Discovery discovers templates that are not found in Prime Infrastructure.
• Existing templates are not discovered.
• Template Discovery does not retrieve dynamic interface configurations for a controller. You must create a new template to apply the dynamic interface configurations on a controller.

Related Topic
• Discovering Controller Templates
• Rebooting Controllers
• Downloading Software to Controllers
• Replacing Old Controller Models with New Models
• Modifying Controller Properties

Discovering Controller Templates

To discover current templates, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click Configure > Discover Templates from Controller.

The Discover Templates page displays the number of discovered templates, each template type and each template name.

Step 4 Select the Enabling this option will create association between discovered templates and the device listed above check box so that discovered templates are associated to the configuration on the device and are shown as applied on that controller.

The template discovery refreshes the configuration from the controller prior to discovering templates.

Step 5 Click OK in the warning dialog box to continue with the discovery.

For the TACACS+ Server templates, the configuration on the controller with same server IP address and port number but different server types are aggregated into one single template with the corresponding Server Types set on the Discovered Template. For the TACACS+ Server templates, the Admin Status on the discovered template reflects the value of Admin Status on the first configuration from the controller with same Server IP address and port number.

Related Topic
• Managing Controller Templates

Viewing Templates Applied to Controllers

You can view all templates currently applied to a specific controller. Prime Infrastructure displays templates applied in the partition only.

To view applied templates, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Chapter 27  Configuring Wireless Devices

Configuring Controllers

Step 2  Select the check box(es) of the applicable controller(s).

Step 3  Click Configure > Templates Applied to a Controller.  
The page displays each applied template name, template type, the date the template was last saved, and the date the template was last applied.

Step 4  Click the template name link to view the template details. See the Managing Controller Templates for more information.

Related Topic
- Auditing Controllers
- Replacing Old Controller Models with New Models

Replacing Old Controller Models with New Models

When you want to replace an old controller model with a new one without changing the IP address, do the following:

1. Delete the old controller from Prime Infrastructure and wait for the confirmation that the device was deleted.
2. Replace the controller with the new model in the setup with same IP address.
3. Re-add the IP address to Prime Infrastructure.

Related Topic
- Modifying Controller Properties

Modifying Controller Properties

To change controller properties such as the device name, location, SNMP parameters, or Telnet/SSH parameters, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2  Select a wireless controller, then click Edit.
Step 3  Modify the fields as desired, then click one of the following buttons:
- Update
- Update & Sync
- Verify Credentials
- Cancel to return to the previous or default settings.

Related Topic
- Configuring Controller System Parameters
Configuring Controller System Parameters

This section describes how to configure the controller system parameters and contains the following topics:

- Modifying General System Properties for Controllers
- Related Topics
- Setting Controller Time and Date

Modifying General System Properties for Controllers

To view the general system parameters for a current controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click a Device Name, then click the Configuration tab.
Step 3 From the left sidebar menu, choose System > General - System. The general system parameters appear.
Step 4 Make the required changes, then click Save.

Related Topic
- Wireless Controllers > System > General - System Field Descriptions

Enabling AP Failover Priority

When a controller fails, the backup controller configured for the access point suddenly receives a number of Discovery and Join requests. If the controller becomes overloaded, it might reject some of the access points.

By assigning failover priority to an access point, you have some control over which access points are rejected. When the backup controller is overloaded, join requests of access points configured with a higher priority levels take precedence over lower-priority access points.

To configure failover priority settings for access points, you must first enable the AP Failover Priority feature.

To enable the AP Failover Priority feature, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click a Device Name, then click the Configuration tab.
Step 3 From the left sidebar menu, choose General - System.
Step 4 From the AP Failover Priority drop-down list, choose Enabled.

Configuring AP Failover Priority

To configure an access point failover priority, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select an AP Name.
Step 2 From the AP Failover Priority drop-down list, choose the applicable priority (Low, Medium, High, Critical). The default priority is Low.

Configuring 802.3 Bridging

The controller supports 802.3 frames and applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP. Only this raw 802.3 frame format is currently supported.

To configure 802.3 bridging using Prime Infrastructure, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click a Device Name, then click the Configuration tab.
Step 3 Choose System > General - System to access the General page.
Step 4 From the 802.3 Bridging drop-down list, choose Enable to enable 802.3 bridging on your controller or Disable to disable this feature. The default value is Disable.
Step 5 Click Save to confirm your changes.

802.3x Flow Control

Flow control is a technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

By default, flow control is disabled. You can only enable a Cisco switch to receive PAUSE frames but not to send them.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click a Device Name, then click the Configuration tab.
Step 3 Choose System > General - System to access the General page.
Step 4 Click Enable in the 802.3x Flow Control field.

Configuring Lightweight Access Point Protocol Transport Mode

Lightweight Access Point Protocol transport mode indicates the communications layer between controllers and access points. Cisco IOS-based lightweight access points do not support Layer 2 lightweight access point mode. These access points can only be run with Layer 3.

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 lightweight access point transport mode using Prime Infrastructure user interface, follow these steps. This procedure causes your access points to go offline until the controller reboots and the associated access points reassociate to the controller.
Configuring Controllers

Chapter 27  Configuring Wireless Devices

Step 1  Make sure that all controllers and access points are on the same subnet.
You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

Step 2  Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 3  Click a Device Name, click the Configuration tab, then choose System > General - System to access the General page.
   a. Change lightweight access point transport mode to Layer2 and click Save.
   b. If Prime Infrastructure displays the following message, click OK:
      Please reboot the system for the CAPWAP Mode change to take effect.

Step 4  Select the controller, then click Reboot > Reboot Controllers.

Step 5  Select the Save Config to Flash option.

Step 6  After the controller reboots, follow these steps to verify that the CAPWAP transport mode is now Layer 2:
   a. Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
   b. Click the device name of the applicable controller.
   c. Verify that the current CAPWAP transport mode is Layer2 from the System > General - System page.

You have completed the CAPWAP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

Aggressive Load Balancing

In routing, load balancing refers to the capability of a router to distribute traffic over all its network ports that are the same distance from the destination address. Good load-balancing algorithms use both line speed and reliability information. Load balancing increases the use of network segments, thus increasing effective network bandwidth.

Aggressive load balancing actively balances the load between the mobile clients and their associated access points.

Link Aggregation

Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG). In a 4402 model, two ports are combined to form a LAG whereas in a 4404 model, all four ports are combined to form a LAG.

You cannot create more than one LAG on a controller.

If LAG is enabled on a controller, the following configuration changes occur:
   • Any dynamic interfaces that you have created are deleted in order to prevent configuration inconsistencies in the interface database.
   • Interfaces cannot be created with the “Dynamic AP Manager” flag set.

The advantages of creating a LAG include the following:
• Assurance that, if one of the links goes down, the traffic is moved to the other links in the LAG. As long as one of the physical ports is working, the system remains functional.
• You do not need to configure separate backup ports for each interface.
• Multiple AP-manager interfaces are not required because only one logical port is visible to the application.

When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

**Wireless Management**

Because of IPsec operation, management via wireless is only available to operators logging in across WPA, Static WEP, or VPN Pass Through WLANs. Wireless management is not available to clients attempting to log in via an IPsec WLAN.

**Mobility Anchor Group Keep Alive Interval**

You can specify the delay between tries for clients attempting to join another access point. This decreases the time it takes for a client to join another access point following a controller failure because the failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

**Related Topics**
- Restoring Controller Factory Defaults
- Setting Controller Time and Date
- Downloading Configurations to Controllers

**Restoring Controller Factory Defaults**

You can reset the controller configuration to the factory default. This overwrites all applied and saved configuration parameters. You are prompted for confirmation to reinitialize your controller.

All configuration data files are deleted, and upon reboot, the controller is restored to its original non-configured state. This removes all IP configuration, and you need a serial connection to restore its base configuration.

---

**Step 1** Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

**Step 2** Click a Device Name, then click the Configuration tab.

**Step 3** From the left sidebar menu, choose System > Commands, and from the Administrative Commands drop-down list, choose Reset to Factory Default, and click Go to access this page.

**Step 4** After confirming configuration removal, you must reboot the controller and select the Reboot Without Saving option.

---

**Related Topic**
- Rebooting Controllers
- Setting Controller Time and Date
- Downloading Configurations to Controllers
Setting Controller Time and Date

You can manually set the current time and date on the controller.

Step 1
Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2
Click a Device Name, then click the Configuration tab.

Step 3
From the left sidebar menu, choose System > Commands, and from the Configuration Commands drop-down list choose Set System Time, and click Go.

Step 4
Modify the required parameters:
- Current Time—Shows the time currently being used by the system.
- Month/Day/Year—Choose the month/day/year from the drop-down list.
- Hour/Minutes/Seconds—Choose the hour/minutes/seconds from the drop-down list.
- Delta (hours)—Enter the positive or negative hour offset from GMT (Greenwich Mean Time).
- Delta (minutes)—Enter the positive or negative minute offset from GMT.
- Daylight Savings—Select to enable Daylight Savings Time.

Uploading Configuration and Logs from Controllers

You can upload files from controllers to a local TFTP (Trivial File Transfer Protocol) server. You must enable TFTP to use the Default Server option on the Administration System Settings > Server Settings page.

Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Cisco Prime Infrastructure and the third-party TFTP servers use the same communication port.

Step 1
Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2
Click a Device Name, then click the Configuration tab.

Step 3
From the left sidebar menu, choose System > Commands.

Step 4
From the Upload/Download Commands drop-down list, choose Upload File from Controller, then click Go.

By default, configuration file encryption is disabled. Uploading configuration file is unsecured without encryption.

Step 5
To enable encryption before uploading files, click the link at the bottom of the Upload File from Controller page.

Step 6
Complete the required fields, then click OK. The selected file is uploaded to your TFTP server with the name you specified.

Related Topic
- Downloading Configurations to Controllers
- Restoring Controller Factory Defaults
Chapter 27     Configuring Wireless Devices

Configuring Controllers

- Setting Controller Time and Date
- Downloading Configurations to Controllers

**Downloading Configurations to Controllers**

You can download configuration files to your controller from a local TFTP (Trivial File Transfer Protocol) server.

Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Cisco Prime Infrastructure and the third-party TFTP servers use the same communication port.

---

**Step 1** Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.
**Step 2** Click a Device Name, then click the **Configuration** tab.
**Step 3** From the left sidebar menu, choose **System > Commands**.
**Step 4** From the Upload/Download Commands drop-down list, choose **Download Config**, then click **Go**.
**Step 5** Complete the required fields, then click **OK**.

---

**Related Topic**
- Uploading Configuration and Logs from Controllers
- Restoring Controller Factory Defaults
- Setting Controller Time and Date

**Downloading Icons to Controllers**

You can download configuration files to your controller from a local TFTP (Trivial File Transfer Protocol) server. Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Cisco Prime Infrastructure and the third-party TFTP servers use the same communication port.

---

**Step 1** Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.
**Step 2** Click a Device Name, then click the **Configuration** tab.
**Step 3** From the left sidebar menu, choose **System > Commands**.
**Step 4** From the Upload/Download Commands drop-down list, choose **Download Config**, and click **Go**.
**Step 5** Complete the required fields, then click **OK**.

---

**Related Topic**
- Downloading Configurations to Controllers
- Restoring Controller Factory Defaults
- Setting Controller Time and Date
• Downloading Configurations to Controllers

Configuring Controller System Interfaces

Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller to configure controller system interfaces.

Related Topics
• Adding Interfaces to Controllers
• Viewing or Modifying Controller Interface Details
• Deleting Dynamic Interfaces
• NAC Integration
• Wired Guest Access

Adding Interfaces to Controllers

To add an interface:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click a Device Name, then click the Configuration tab.
Step 3 From the left sidebar menu, choose System > Interfaces.
Step 4 From the Select a command drop-down list, choose Add Interface > Go.
Step 5 Complete the required fields, then click Save.

Related Topics
• Viewing or Modifying Controller Interface Details
• Deleting Dynamic Interfaces

Viewing or Modifying Controller Interface Details

To view the existing interfaces:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click a Device Name, then click the Configuration tab.
Step 3 From the left sidebar menu, choose System > Interfaces. The following parameters appear:
  • Check box—Check box to select the dynamic interface for deletion. Choose Delete Dynamic Interfaces from the Select a command drop-down list.
  • Interface Name —User-defined name for the interface (for example, Management, Service-Port, Virtual).
Configuring Controllers

- VLAN Id—VLAN identifier between 0 (untagged) and 4096, or N/A.
- Quarantine—Select the check box if the interface has a quarantine VLAN ID configured on it.
- IP Address—IP address of the interface.
- Interface Type—Interface Type: Static (Management, AP-Manager, Service-Port, and Virtual interfaces) or Dynamic (operator-defined interfaces).
- AP Management Status—Status of AP Management interfaces and the parameters include Enabled, Disabled, and N/A. Only the management port can be configured as Redundancy Management Interface port.

Related Topics
- Adding Interfaces to Controllers
- Deleting Dynamic Interfaces

Deleting Dynamic Interfaces

The dynamic interface cannot be deleted if it has been assigned to any interface group. To delete a dynamic interface:

Step 1
Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2
Click a Device Name, then click the Configuration tab.

Step 3
From the left sidebar menu, choose System > Interfaces.

Step 4
Select the check box of the dynamic interface that you want to delete and choose Delete Dynamic Interfaces from the Select a command drop-down list.

Step 5
Click OK to confirm the deletion.

Related Topics
- Adding Interface Groups
- Viewing or Modifying Controller Interface Details

Configuring Controller System Interface Groups

Interface groups are logical groups of interfaces. Interface groups facilitate user configuration where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface group can exclusively contain either quarantine or non-quarantine interfaces. An interface can be part of multiple interface groups.

Follow these recommendations while configuring controller system interface groups:
- Ensure that the interface group name is different from the interface name.
- Guest LAN interfaces cannot be part of interface groups

The Interface Groups feature is supported by Cisco Wireless Controller software release 7.0.116.0 and later.
Adding Interface Groups

To add an interface group:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click on a Device Name, then click the Controller tab.

**Step 3** From the left sidebar menu, choose System > Interface Groups.

**Step 4** From the Select a command drop-down list, choose Add Interface Group and click Go.

**Step 5** Complete the required fields, then click Add.

The Interface dialog box appears.

**Step 6** Select the interfaces that you want to add to the group, and click Select.

**Step 7** To remove an Interface from the Interface group, from the Interface Group page, select the Interface and click Remove.

**Step 8** Click Save to confirm the changes made.

Deleting Interface Groups

You cannot delete interface groups that are assigned to:

- WLANs
- AP groups
- Foreign Controller Mapping for WLANs
- WLAN templates
- AP group templates

To delete an interface group:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click on a Device Name, then click the Controller tab.

**Step 3** Click the Device Name of the applicable controller.

**Step 4** From the left sidebar menu, choose System > Interface Groups.
Step 5 Select the check box of the interface group that you want to delete.
Step 6 From the Select a command drop-down list, choose **Delete Interface Group**, and click **Go**.
Step 7 Click **OK** to confirm the deletion.

**Related Topics**
- Configuring Controller System Interface Groups

**Viewing Interface Groups**

To view existing interface groups:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Devices Groups menu on the left, select **Device Type > Wireless Controller**.
Step 2 Click on a Device Name, then click the **Controller** tab.
Step 3 From the left sidebar menu, choose **System > Interface Groups**. The following parameters appear:
  - **Name**—User-defined name for the interface group (For example, group1, group2).
  - **Description**—(Optional) Description for the Interface Group.
  - **Interfaces**—Count of the number of interfaces belonging to the group.
Step 4 Click the **Interface Group Name** link.
The Interface Groups Details page appears with the Interface group details as well as the details of the Interfaces that form part of that particular Interface group.

**Related Topics**
- Configuring Controller System Interface Groups

**NAC Integration**

The Cisco Network Admission Control (NAC) appliance, also known as Cisco Clean Access (CCA), is a Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

**Related Topics**
- Guidelines for Using SNMP NAC
- Configuring NAC Out-of-Band Integration (SNMP NAC): Workflow
Guidelines for Using SNMP NAC

Follow these guidelines when using SNMP NAC out-of-band integration:

- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Therefore, multiple NAC appliances might need to be deployed.
- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN, provided they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
- For posture reassessment based on session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.
- When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. Once the session timeout expires for WLANs using web authentication, clients deauthenticate from the controller and must perform posture validation again.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.
- NAC out-of-band integration is not supported for use with the WLAN AAA override feature.
- All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

Related Topics

- Cisco NAC Appliance Configuration

Guidelines for Using RADIUS NAC

Follow these guidelines when using RADIUS NAC:

- RADIUS NAC is available only for WLAN with 802.1x/WPA/WPA2 Layer 2 security.
- RADIUS NAC cannot be enabled when FlexConnect local switching is enabled.
- AAA override should be enabled to configure RADIUS NAC.

Related Topics

- NAC Integration
Configuring NAC Out-of-Band Integration (SNMP NAC): Workflow

To configure SNMP NAC out-of-band integration, follow this workflow:

1. Configure the quarantine VLAN for a dynamic interface—The NAC appliance supports static VLAN mapping, and you must configure a unique quarantine VLAN for each interface that is configured on the controller.

2. Configure NAC out-of-band support on a WLAN or guest LAN—To enable NAC support on an access point group VLAN, you must first enable NAC on the WLAN or guest LAN.

3. Configure NAC Out-of-band support for a specific AP group—To configure NAC out-of-band support for specific access point groups.

Related Topics
- Configuring Quarantine VLAN for Dynamic Interface
- Configuring NAC Out-of-Band Support on WLANs or Guest LANs
- Configuring NAC Out-of-Band Support for Specific AP Groups

Configuring Quarantine VLAN for Dynamic Interface

To configure the quarantine VLAN for a dynamic interface:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Choose which controller you are configuring for out-of-band integration by clicking it in the IP Address column.

Step 3 Choose System > Interfaces from the left sidebar menu.

Step 4 Click the Interface Name.

Step 5 Choose Add Interface from the Select a command drop-down list and click Go.

Step 6 In the Interface Name text box, enter a name for this interface, such as “quarantine.”

Step 7 In the VLAN ID text box, enter a non-zero value for the access VLAN ID, such as “10.”

Step 8 Select the Quarantine check box if the interface has a quarantine VLAN ID configured on it.

Step 9 Configure any remaining fields for this interface, such as the IP address, netmask, and default gateway.

Note To avoid issues when adding the wireless controller to Prime Infrastructure, the Dynamic Interface should not be in the same subnet as Prime Infrastructure.

Step 10 Enter an IP address for the primary and secondary DHCP server.

Step 11 Click Save.

Related Topics
- Configuring NAC Out-of-Band Support on WLANs or Guest LANs
- Configuring NAC Out-of-Band Support for Specific AP Groups
Configuring NAC Out-of-Band Support on WLANs or Guest LANs

To configure NAC out-of-band support on a WLAN or guest LAN, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click on a Device Name.

**Step 3** Choose WLANs > WLAN from the left sidebar menu.

**Step 4** Choose Add a WLAN from the Select a command drop-down list, and click Go.

**Step 5** If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the click here link to create a new template.

**Step 6** Click the Advanced tab.

**Step 7** To configure SNMP NAC support for this WLAN or guest LAN, choose SNMP NAC from the NAC Stage drop-down list. To disable SNMP NAC support, choose None from the NAC Stage drop-down list, which is the default value.

**Step 8** Click Apply to commit your changes.

**Related Topics**
- Configuring NAC Out-of-Band Support for Specific AP Groups
- Wired Guest Access

Configuring NAC Out-of-Band Support for Specific AP Groups

To configure NAC out-of-band support for a specific AP group, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click on a Device Name, then click the Controller tab.

**Step 3** Choose WLANs > AP Groups VLAN from the left sidebar menu to open the AP Groups page.

**Step 4** Click the name of the desired AP group.

**Step 5** From the Interface Name drop-down list, choose the quarantine enabled interface.

**Step 6** To configure SNMP NAC support for this AP group, choose SNMP NAC from the Nac State drop-down list. To disable NAC out-of-band support, choose None from the Nac State drop-down list, which is the default value.

**Step 7** Click Apply to commit your changes.

**Related Topics**
- Configuring Quarantine VLAN for Dynamic Interface
- Configuring NAC Out-of-Band Support on WLANs or Guest LANs
- Wired Guest Access
Viewing Client State

To see the current state of the client (either Quarantine or Access), follow these steps:

**Step 1** Choose Monitor > Clients and Users to open the Clients. Perform a search for clients.

**Step 2** Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears as access, invalid, or quarantine in the Security Information section.

Related Topics
- Configuring NAC Out-of-Band Integration (SNMP NAC): Workflow

Wired Guest Access

Wired Guest Access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room.

Like wireless guest user accounts, wired guest access ports are added to the network using the Lobby Ambassador feature. Wired Guest Access can be configured in a standalone configuration or in a dual controller configuration employing an anchor and foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired Guest Access ports initially terminate on a Layer 2 access switch or switch port which is configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a wireless LAN controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, a bidirectional Ethernet over IP (EoIP) tunnel is established between the foreign and anchor controllers to handle this traffic.

Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

You can specify how much bandwidth a wired guest user is allocated in the network by configuring and assigning a role and bandwidth contract.

Related Topics
- Configuring and Enabling Wired Guest User Access: Workflow

Configuring and Enabling Wired Guest User Access: Workflow

To configure and enable the wired guest user access, follow this workflow:

1. Configure a dynamic interface (VLAN) for wired guest access—Create a dynamic interface to enable the wired guest user access.
2. Configure a wired LAN for guest user access—Configure a new LAN, which is a guest LAN.
Related Topics

- Configuring a Dynamic Interface for Wired Guest User Access
- Configuring a Wired LAN for Guest User Access

Configuring a Dynamic Interface for Wired Guest User Access

To configure and enable a dynamic interface (VLAN) for wired guest user access on the network:

---

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose System > Interfaces from the left sidebar menu.

Step 4 Choose Add Interface from the Select a command drop-down list, and click Go.

Step 5 Complete the required fields.

Step 6 Click Save.

---

Related Topics

- Configuring and Enabling Wired Guest User Access: Workflow

Configuring a Wired LAN for Guest User Access

To configure a wired LAN for guest user access:

---

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name.

Step 3 To configure a wired LAN for guest user access, choose WLANs > WLAN configuration from the left sidebar menu.

Step 4 Choose Add a WLAN from the Select a command drop-down list, and click Go.

Step 5 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the click here link to create a new template.

Step 6 In the WLAN > New Template general page, enter a name in the Profile Name text box that identifies the guest LAN. Do not use any spaces in the name entered.

Step 7 Select the Enabled check box for the WLAN Status field.

Step 8 From the Ingress Interface drop-down list, choose the VLAN that you created in Step 3. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 9 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic. If you have only one controller in the configuration, choose management from the Egress Interface drop-down list.
Step 10  Click the Security > Layer 3 tab to modify the default security policy (web authentication) or to assign WLAN specific web authentication (login, logout, login failure) pages and the server source.

a. To change the security policy to passthrough, select the **Web Policy** check box and select the **Passthrough** radio button. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

b. To specify custom web authentication pages, unselect the Global WebAuth Configuration **Enabled** check box.

When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

- **Default Internal**—Displays the default web login page for the controller. This is the default value.
- **Customized Web Auth**—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.
- **External**—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

You can select specific RADIUS or LDAP servers to provide external authentication in the **Security > AAA** pane. The RADIUS and LDAP external servers must be already configured to have selectable options in the **Security > AAA** pane. You can configure these servers on the RADIUS Authentication Servers, TACACS+ Authentication Servers page, and LDAP Servers page.

Step 11  If you selected External as the Web Authentication Type, choose **Security > AAA** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Step 12  Click **Save**.

Step 13  Repeat this process if a second (anchor) controller is being used in the network.

**Related Topics**
- Configuring and Enabling Wired Guest User Access: Workflow

---

**Creating an Ingress Interface**

To create an Ingress interface:

Step 1  Choose **Configuration > Network > Network Devices**, then from the Devices Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2  Click on a Device Name, then click the **Controller** tab.

Step 3  Choose **System > Interfaces** from the left sidebar menu.

Step 4  Choose **Add Interface** from the Select a command drop-down list, and click **Go**.

Step 5  In the Interface Name text box, enter a name for this interface, such as **guestinterface**.

Step 6  Enter a VLAN identifier for the new interface.
Step 7 Select the Guest LAN check box.
Step 8 Enter the primary and secondary port numbers.
Step 9 Click Save.

Related Topics
- Creating an Egress Interface

Creating an Egress Interface

To create an Egress interface:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.
Step 2 Click on a Device Name, then click the Controller tab.
Step 3 Choose System > Interfaces from the left sidebar menu.
Step 4 Choose Add Interface from the Select a command drop-down list, and click Go.
Step 5 In the Interface Name text box, enter a name for this interface, such as quarantine.
Step 6 In the vlan Id text box, enter a non-zero value for the access VLAN ID, such as 10.
Step 7 Select the Quarantine check box and enter a non-zero value for the Quarantine VLAN identifier, such as 110.

You can have NAC-support enabled on the WLAN or guest WLAN template Advanced tab for interfaces with Quarantine enabled.
Step 8 Enter the IP address, Netmask, and Gateway information.
Step 9 Enter the primary and secondary port numbers.
Step 10 Provide an IP address for the primary and secondary DHCP server.
Step 11 Configure any remaining fields for this interface, and click Save.

You are now ready to create a wired LAN for guest access.

Related Topics
- Creating an Ingress Interface

Configuring Controller Network Routes

The Network Route page enables you to add a route to the controller service port. This route allows you to direct all Service Port traffic to the designated management IP address.

Related Topics
- Viewing Existing Network Routes
- Adding Network Routes
Viewing Existing Network Routes

To view existing network routes:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click on a Device Name, then click the Controller tab.
Step 3 Choose System > Network Route from the left sidebar menu. The following parameters appear:
  - IP Address—The IP address of the network route.
  - IP Netmask—Network mask of the route.
  - Gateway IP Address—Gateway IP address of the network route.

Related Topics
- Configuring Controller Network Routes

Adding Network Routes

To add a network route, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click on a Device Name, then click the Controller tab.
Step 3 Choose System > Network Route from the left sidebar menu.
Step 4 From the Select a command drop-down list, choose Add Network Route.
Step 5 Click Go.
Step 6 Complete the required fields, then click Save.

Related Topics
- Configuring Controller Network Routes

Viewing Controller Spanning Tree Protocol Parameters

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view or manage current STP parameters:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click on a Device Name, then click the Controller tab.
Step 3  Choose System > Spanning Tree Protocol from the left sidebar menu. The Spanning Tree Protocol page displays the following parameters:

- Protocol Spec—The current protocol specification.
- Admin Status—Select this check box to enable.
- Priority—The numerical priority number of the ideal switch.
- Maximum Age (seconds)—The amount of time (in seconds) before the received protocol information recorded for a port is discarded.
- Hello Time (seconds)—Determines how often (in seconds) the switch broadcasts its hello message to other switches.
- Forward Delay (seconds)—The time spent (in seconds) by a port in the learning/listening states of the switches.

Related Topics
- Configuring Controller Network Routes
- Configuring Controller System Parameters

Configuring Controller Mobility Groups

By creating a mobility group, you can enable multiple network controllers to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of client devices and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy.

If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

Related Topics
- Messaging Among Mobility Groups
- Mobility Group Prerequisites
- Viewing Current Mobility Group Members
- Adding Mobility Group Members from a List of Controllers
- Manually Adding Mobility Group Members
- Setting the Mobility Scalability Parameters

Messaging Among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers:

- There can be up to 72 members in the list with up to 24 in the same mobility group.
- The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it.
- In Prime Infrastructure and Wireless Controller software release 5.0 and later, the controller uses multicast mode to send the Mobile Announce messages. This allows the controller to send only one copy of the message to the network, which delivers it to the multicast group containing all the mobility members.

**Related Groups**
- Configuring Controller Mobility Groups

**Mobility Group Prerequisites**

Before you add controllers to a mobility group, you must verify that the following prerequisites are met for all controllers that are to be included in the group:

- All controllers must be configured for the same CAPWAP transport mode (Layer 2 or Layer 3).
- IP connectivity must exist between the management interfaces of all controllers.
- All controllers must be configured with the same mobility group name.
- All controllers must be configured with the same virtual interface IP address.
- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.

**Related Groups**
- Configuring Controller Mobility Groups

**Viewing Current Mobility Group Members**

To view current mobility group members:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click on a Device Name, then click the Controller tab.

**Step 3** Choose System > Mobility Groups from the left sidebar menu.

**Related Groups**
- Adding Mobility Group Members from a List of Controllers
- Manually Adding Mobility Group Members

**Adding Mobility Group Members from a List of Controllers**

To add a mobility group member from a list of existing controllers:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click on a Device Name, then click the Controller tab.

**Step 3** Choose System > Mobility Groups from the left sidebar menu.
Step 4 From the Select a command drop-down list, choose Add Group Members.

Step 5 Click Go.

Step 6 Select the check box(es) for the controller to be added to the mobility group.

Step 7 Click Save.

Related Groups
- Viewing Current Mobility Group Members
- Manually Adding Mobility Group Members

Manually Adding Mobility Group Members

If there were no controllers found to add to the mobility group, you can add members manually. To manually add members to the mobility group, follow these steps:

Step 1 Click the click here link from the Mobility Group Member details page.

Step 2 In the Member MAC Address text box, enter the MAC address of the controller to be added.

Step 3 In the Member IP Address text box, enter the management interface IP address of the controller to be added.

If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the controller management interface IP address. Otherwise, mobility fails among controllers in the mobility group.

Step 4 Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The local mobility member group address must be the same as the local controller group address.

Step 5 In the Group Name text box, enter the name of the mobility group.

Step 6 Click Save.

Step 7 Repeat Steps 1 through 6 for the remaining Cisco Wireless Controller devices.

Related Topics
- Adding Mobility Group Members from a List of Controllers
- Viewing Current Mobility Group Members

Setting the Mobility Scalability Parameters

Before You Begin
You must configure Mobility Groups prior setting up the mobility scalability parameters.

To set the mobility message parameters:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the Device Name of a controller whose software version is 5.0 or later.
Chapter 27 Configuring Wireless Devices

### Configuring Controllers

Step 3 From the left sidebar menu, choose **System > General**.

Step 4 From the Multicast Mobility Mode drop-down list, specify if you want to enable or disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members.

Step 5 If you enabled multicast messaging by setting multicast mobility mode to enabled, you must enter the group IP address at the Mobility Group Multicast-address field to begin multicast mobility messaging. You must configure this IP address for the local mobility group but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

Step 6 Click **Save**.

### Related Topics
- Configuring Controller Multicast Mode
- Configuring Controller System Parameters

### Configuring Controller Network Time Protocol

To add a new NTP Server:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Devices Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose **System > Network Time Protocol**.

Step 4 From the Select a command drop-down list, choose **Add NTP Server**.

Step 5 Click **Go**.

Step 6 From the Select a template to apply to this controller drop-down list, choose the applicable template to apply to this controller.

### Related Topics
- Configuring Controller System Parameters
- Configuring Controller Network Time Protocol

### Background Scanning on 1510s in Mesh Networks

Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. Because the access points are searching on neighboring channels as well as the current channel, the list of optimal alternate paths and parents is greater.

Identifying this information prior to the loss of a parent results in a faster transfer and the best link possible for the access points. Additionally, access points might switch to a new channel if a link on that channel is found to be better than the current channel in terms of fewer hops, stronger signal-to-noise ratio (SNR), and so on.
Background scanning on other channels and data collection from neighbors on those channels are performed on the primary backhaul between two access points:

The primary backhaul for 1510s operate on the 802.11a link.

Background scanning is enabled on a global basis on the associated controller of the access point. Latency might increase for voice calls when they are switched to a new channel.

In the EMEA regulatory domain, locating neighbors on other channels might take longer given DFS requirements.

**Related Topics**
- Background Scanning Scenarios
- Enabling Background Scanning

**Background Scanning Scenarios**

A few scenarios are provided below to better illustrate how background scanning operates.

In Figure 27-1, when the mesh access point (MAP1) initially comes up, it is aware of both root access points (RAP1 and RAP2) as possible parents. It chooses RAP2 as its parent because the route through RAP2 is better in terms of hops, SNR, and so on. After the link is established, background scanning (once enabled) continuously monitors all channels in search of a more optimal path and parent. RAP2 continues to act as parent for MAP1 and communicates on channel 2 until either the link goes down or a more optimal path is located on another channel.

**Figure 27-1  Mesh Access Point (MAP1) Selects a Parent**

![Diagram of mesh access point (MAP1) selecting a parent](Diagram)

In Figure 27-2, the link between MAP1 and RAP2 is lost. Data from ongoing background scanning identifies RAP1 and channel 1 as the next best parent and communication path for MAP1 so that link is established immediately without the need for additional scanning after the link to RAP2 goes down.
Enabling Background Scanning

To enable background scanning on an AP1510 RAP or MAP:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click an IP address of the applicable controller.

Step 3 Choose Mesh > Mesh Settings from the left sidebar menu.

Step 4 Select the Background Scanning check box to enable background scanning or unselect it to disable the feature. The default value is disabled.

Step 5 This feature eliminates the time consuming task of finding a parent across channels by scanning all the channels. The off-channel procedure transmits broadcast packets on selected channels (at a periodicity of 3 seconds, with a maximum of 50 milliseconds per off-channel) and receives packets from all 'reachable' neighbors. This keeps the child MAP updated with neighbor information across channels enabling it to 'switch' to a new neighbor and use it as a parent for the uplink. The 'switch' need not be triggered from parent loss detection, but on identifying a better parent while the child MAP still has its current parent uplink active.

Step 6 Click Save.

Related Topics
- Background Scanning Scenarios
Configuring Controller QoS Profiles

To make modifications to the quality of service profiles:

**Step 1**  Choose **Configuration > Network > Network Devices**, then from the Devices Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2**  Click an IP address of the applicable controller.

**Step 3**  From the left sidebar menu, choose **System > QoS Profiles**. The following parameters appear:

- Bronze—For Background
- Gold—For Video Applications
- Platinum—For Voice Applications
- Silver—For Best Effort

**Step 4**  Click the applicable profile to view or edit profile parameters.

**Step 5**  Click **Save**.

**Related Topics**
- Configuring Controller System Parameters

Configuring Controller DHCP Scopes

Controllers have built-in DHCP relay agents. However, when you desire network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes that assign IP addresses and subnet masks to wireless client. Typically, one controller can have one or more DHCP scopes that each provide a range of IP addresses.

**Related Topics**
- Viewing Current DHCP Scopes
- Adding a New DHCP Scope

Viewing Current DHCP Scopes

To view current DHCP (Dynamic Host Configuration Protocol) scopes, follow these steps:

**Step 1**  Choose **Configuration > Network > Network Devices**, then from the Devices Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2**  Click the Device Name of the applicable controller.

**Step 3**  From the left sidebar menu, choose **System > DHCP Scopes**.

**Related Topics**
- Configuring Controller DHCP Scopes
Adding a New DHCP Scope

To add a new DHCP Scope, follow these steps:

---

**Step 1**  Choose **Configuration > Network > Network Devices**, then from the Devices Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2**  Click the Device Name of the applicable controller.

**Step 3**  From the left sidebar menu, choose **System > DHCP Scopes**.

**Step 4**  From the Select a command drop-down list, choose **Add DHCP Scope** and click **Go**.

**Step 5**  Configure the required fields, and click **Save**.

---

**Related Topics**
- Configuring Controller DHCP Scopes
- Configuring Controller System Parameters

Viewing Controller User Roles

To view current local net user roles on a controller, follow these steps:

---

**Step 1**  Choose **Configuration > Network > Network Devices**, then from the Devices Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2**  Click the Device Name of the applicable controller.

**Step 3**  From the left sidebar menu, choose **System > User Roles**.

The Local Net User Role parameters appear.

**Step 4**  Click a Template Name to view the User Role details.

---

**Related Topics**
- Adding a New Local Net User Role to Controllers

Adding a New Local Net User Role to Controllers

To add a new local net user role to a controller:

---

**Step 1**  Choose **Configuration > Network > Network Devices**, then from the Devices Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2**  Click the Device Name of the applicable controller.

**Step 3**  From the left sidebar menu, choose **System > User Roles**.

**Step 4**  From the Select a command drop-down list, choose **Add User Role**.

**Step 5**  Select a template from the Select a template to apply to this controller drop-down list.
Step 6 Click Apply.

Related Topics
- Adding a New Local Net User Role to Controllers
- Configuring Controller System Parameters

**Configuring a Global Access Point Password**

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To establish a global username and password, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

**Step 2** Click the Device Name of a controller with a Release 5.0 or later.

**Step 3** From the left sidebar menu, choose System > AP Username Password.

**Step 4** Enter the username and password that you want to be inherited by all access points that join the controller.

For Cisco IOS access points, you must also enter and confirm an enable password.

**Step 5** Click Save.

**Configuring Global CDP**

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

CDP is enabled on the Ethernet and radio ports of a bridge by default.

Global Interface CDP configuration is applied to only the APs with CDP enabled at AP level.

To configure a Global CDP, perform the following steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

**Step 2** Click the Device Name of the desired controller.

**Step 3** From the left sidebar menu, choose System > Global CDP Configuration from the left sidebar menu. The Global CDP Configuration page appears.
Configuring Wireless Devices

Chapter 27  Configuring Wireless Devices

Configuring Controllers

Step 4 Configure the required fields in the Global CDP Configuration page. In the Global CDP group box, configure the following parameters:

- CDP on controller—Choose enable or disable CDP on the controller. This configuration cannot be applied on WiSM2 controllers.
- Global CDP on APs—Choose to enable or disable CDP on the access points.
- Refresh-time Interval (seconds)—In the Refresh Time Interval field, enter the time in seconds at which CDP messages are generated. The default is 60.
- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 5 In the CDP for Ethernet Interfaces group box, select the slots of Ethernet interfaces for which you want to enable CDP.

CDP for Ethernet Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 6 In the CDP for Radio Interfaces group box, select the slots of Radio interfaces for which you want to enable CDP.

CDP for Radio Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 7 Click Save.

Related Topic

- Configuring Controller System Parameters

Configuring AP 802.1X Supplicant Credentials

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future.

If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

To enable global supplicant credentials, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose System > AP 802.1X Supplicant Credentials.

Step 4 Select the Global Supplicant Credentials check box.

Step 5 Enter the supplicant username.

Step 6 Enter and confirm the applicable password.

Step 7 Click Save. Once saved, you can click Audit to perform an audit on this controller.
Configuring Controller DHCP

To configure DHCP (Dynamic Host Configuration Protocol) information for a controller:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose System > DHCP.

Step 4 Add or modify the following parameters:

- DHCP Option 82 Remote Id Field Format—Choose AP-MAC, AP-MAC-SSID, AP-ETHMAC, or AP-NAME-SSID from the drop-down list.
  To set the format for RemoteID field in DHCP option 82
  If Ap-Mac is selected, then set the RemoteID format as AP-Mac. If Ap-Mac-ssid is selected, then set the RemoteID format as AP-Mac:SSID.

- DHCP Proxy—Select the check box to enable DHCP by proxy.
  When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

Step 5 Enter the DHCP Timeout in seconds after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds. DHCP Timeout is applicable for Controller Release 7.0.114.74 and later.

Step 6 Click Save.

Once saved, you can click Audit to perform an audit on this controller.

Related Topics
- Configuring Controller System Parameters

Configuring Controller Multicast Mode

Prime Infrastructure provides an option to configure IGMP (Internet Group Management Protocol) snooping and timeout values on the controller.

IGMP

To configure multicast mode and IGMP snooping for a controller:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose System > Multicast.
Step 4  From the Ethernet Multicast Support drop-down list, choose the applicable Ethernet multicast support (Unicast or Multicast).

Step 5  If Multicast is selected, enter the multicast group IP address.

Step 6  Select the Global Multicast Mode check box to make the multicast mode available globally.

IGMP Snooping and timeout can be set only if Ethernet Multicast mode is Enabled. Select to enable IGMP Snooping.

Step 7  Choose Enable from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.

Step 8  If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

Step 9  Select the Multicast Direct check box to enable videos to be streamed over a wireless network.

Step 10  Choose Enable from the Multicast Mobility Mode drop-down list to change MLD configuration.

Step 11  Select the Enable MLD Snooping check box to enable IPv6 MLD snooping. If you have selected this check box, configure the following parameters:

- MLD Timeout—Enter the MLD timeout value in seconds. The timeout has a range of 3 to 7200 and a default value of 60.

- MLD Query Interval—Enter the MLD query interval timeout value in seconds. The interval has a range of 15 to 2400 and a default value of 20.

Internet Group Management Protocol (IGMP) snooping enables you to limit the flooding of multicast traffic for IPv4. For IPv6, Multicast Listener Discovery (MLD) snooping is used.

Step 12  Configure the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

Step 13  Click Save.

Once saved, you can click Audit to perform an audit on this controller.

Related Topics
- Configuring Controller System Parameters

Configuring Access Point Timer Settings

Advanced timer configuration for FlexConnect and local mode is available for the controller on Prime Infrastructure.

This feature is only supported on Release 6.0 controllers and later.

Related Topics
- Configuring Advanced Timers
Configuring Advanced Timers

To configure the advanced timers, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Choose the controller for which you want to set timer configuration.

**Step 3** From the left sidebar menu, choose System > AP Timers.

**Step 4** In the AP Timers page, click the applicable Access Point Mode link: Local Mode or FlexConnect Mode.

**Step 5** Configure the necessary parameters in the Local Mode AP Timer Settings page or in the FlexConnect Mode AP Timer Settings page accordingly.

- **AP timer settings for Local Mode**—To reduce the failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller. You can then enter a value between 10 and 15 seconds.

- **AP timer settings for FlexConnect**—Once selected, you can configure the FlexConnect timeout value. Select the AP Primary Discovery Timeout check box to enable the timeout value. Enter a value between 30 and 3600 seconds. 5500 series controllers accept access point fast heartbeat timer values in the range of 1-10.

**Step 6** Click Save.

**Related Topics**
- Configuring Access Point Timer Settings

Configuring Controller WLANs

Because controllers can support 512 WLAN configurations, Prime Infrastructure provides an effective way to enable or disable multiple WLANs at a specified time for a given controller.

To view a summary of the wireless local access networks (WLANs) that you have configured on your network, follow these steps:

**Step 1** Choose Configure > Controllers.

**Step 2** Click the Device Name of the applicable controller.

**Step 3** From the left sidebar menu, choose WLANs > WLAN Configuration.

**Step 4** Configure the required fields in the Configure WLAN Summary page appears.

**Related Topics**
- Configuring Controller WLANs
Configuring Controller WLANs

Because controllers can support 512 WLAN configurations, Prime Infrastructure provides an effective way to create WLANs on controllers, and enable or disable multiple WLANs at a specified time for a given controller.

Related Topics
- Viewing Controller WLAN Configurations
- Adding Policies to Controller WLANs
- Configuring Mobile Concierge (802.11u) on WLANs
- Adding WLANs to Controllers
- Deleting Controller WLANs
- Scheduling Status Changes for Multiple Controller WLANs
- Viewing WLAN Mobility Anchors
- Working with WLAN AP Groups

Viewing Controller WLAN Configurations

Step 1  Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2  Click the Device Name of the wireless controller whose WLAN configurations you want to see.
Step 3  Click the Configuration tab.
Step 4  Under Features, choose WLANs > WLAN Configuration. The WLAN Configuration summary page appears, displaying the list of WLANs currently configured on the controller, including each:
  - WLAN ID
  - The name of the WLAN configuration profile
  - WLAN SSID
  - The names of any active security policies
  - The WLAN current administrative status (enabled or disabled)
  - A link to the list of all currently scheduled WLAN configuration tasks
Step 5  To view WLAN configuration details, click the WLAN ID. The WLAN Configuration details page appears.
Step 6  Use the tabs (General, Security, QoS, and Advanced) to view or edit parameters for the WLAN. Whenever you change a parameter, click Save.

Related Topics
- Adding Policies to Controller WLANs
- Configuring Mobile Concierge (802.11u) on WLANs
- Adding WLANs to Controllers
- Deleting Controller WLANs
Adding Policies to Controller WLANs

Step 1
Click Add Row.

Step 2
Select a policy name that you want to map to the WLAN, from the drop-down list.

Step 3
Enter the priority. The priority ranges from 1 to 16.
Two policies cannot have the same priority.

Step 4
Click Save.
If you want to delete a policy, select the check box corresponding to the policy that you want to delete and click Delete.

Related Topics
- Viewing Controller WLAN Configurations
- Configuring Mobile Concierge (802.11u) on WLANs
- Adding WLANs to Controllers
- Deleting Controller WLANs
- Scheduling Status Changes for Multiple Controller WLANs
- Viewing WLAN Mobility Anchors

Configuring Mobile Concierge (802.11u) on WLANs

Cisco Mobile Concierge is a solution that enables 802.1X-capable clients to interwork with external networks without pre-authorization. Mobile Concierge provides service availability information to clients that can help them to associate to available networks more quickly, easily, and securely.

The services offered by the network can be broadly classified into two protocols:
- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:
- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

Step 1
Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2
Click the Device Name of the wireless controller on which you want to configure Mobile Concierge.

Step 3
Click the Configuration tab.

Step 4
Under Features, choose WLANs > WLAN Configuration. The WLAN Configuration summary page appears, displaying the list of WLANs currently configured on the controller,
Step 5  Click the WLAN ID of the WLAN on which you want to configure Mobile Concierge.

Step 6  Click the Hot Spot tab.

Step 7  Click the **802.11u Configuration** sub-tab and complete the fields as follows:

a. Select the **802.11u Status** check box to enable 802.11u on the WLAN.

b. Select the **Internet Access** check box to enable this WLAN to provide Internet services.

c. From the **Network Type** drop-down list, choose the appropriate description for the 802.11u service you want to configure on this WLAN. The following options are available:

   - Private Network
   - Private Network with Guest Access
   - Chargeable Public Network
   - Free Public Network
   - Emergency Services Only Network
   - Personal Device Network
   - Test or Experimental
   - Wildcard

d. Choose the authentication type that you want to configure for the 802.11u parameters on this network:

   - Not configured
   - Acceptance of Terms and Conditions
   - Online Enrollment
   - DNS Redirection
   - HTTP/HTTPS Redirection

e. In the **HESSID** field, enter the Homogeneous Extended Service Set Identifier value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

f. In the **IPv4 Address Type** field, choose the method of assigning IPv4 addresses:

   - Not Available
   - Public
   - Port Restricted
   - Single NAT Private
   - Double NAT Private
   - Port Restricted and Single NAT Private
   - Port Restricted and Double NAT Private
   - Unknown

g. In the **IPv6 Address Type** field, choose the method of assigning IPv6 addresses:

   - Not Available
   - Available
   - Unknown
Step 8  Click the **Others** sub-tab and complete the fields as follows:

a. In the OUI List group box, click **Add Row** and enter the following details:
   - OUI name
   - Is Beacon
   - OUI Index

Click **Save** to add the OUI (Organizationally Unique Identifier) entry to this WLAN.

b. In the Domain List group box, click **Add Row** and enter the following details:
   - Domain Name—The domain name operating in the 802.11 access network.
   - Domain Index—Choose the domain index from the drop-down list.

Click **Save** to add the domain entry to this WLAN.

c. In the Cellular section, click **Add Row** and enter the following details:
   - Country Code—The 3-character cellular country code.
   - Network Code—The 3-character cellular network code.

Click **Save** to add the cellular entry to this WLAN.

Step 9  Click the **Realm** sub-tab and complete the fields as follows:

a. Click **Add Row** and enter the realm name.

b. Click **Save** to add the realm entry to this WLAN.

Step 10 Click the **Service Advertisements** sub-tab and complete the fields as follows:

a. Select the **MSAP Enable** check box to enable service advertisements.

b. If you enable MSAP, enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.

MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers. Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.

c. In the Operator Name List, click **Add Row** and enter the following details:
   - Operator Name—Specify the name of the 802.11 operator.
   - Operator Index—Select an operator index. The range is from 1 to 32.

Step 11 Click the **Hotspot 2.0** sub-tab and complete the fields as follows:

a. Choose the **Enable** option from the HotSpot2 Enable drop-down list.

b. In the WAM Metrics group box, specify the following:
   - WAN Link Status—The link status. The valid range is 1 to 3.
   - WAN SIM Link Status—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
   - Down Link Speed—The downlink speed. The maximum value is 4,194,304 kbps.
   - Up Link Speed—The uplink speed. The maximum value is 4,194,304 kbps.
Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code.

Click Save to add the operator to the list.

In the Port Config List, click Add Row and enter the following details:

- IP Protocol—The IP protocol that you want to enable. The following options are ESP, FTP, ICMP, and IKEV2.
- Port No—The port number that is enabled on this WLAN.
- Status—The status of the port.

Click Save to add the port configuration to the list.

Step 12 Click Save to save the Mobile Concierge configuration.

Related Topics
- Viewing Controller WLAN Configurations
- Adding Policies to Controller WLANs
- Adding WLANs to Controllers
- Deleting Controller WLANs
- Scheduling Status Changes for Multiple Controller WLANs
- Viewing WLAN Mobility Anchors

Adding WLANs to Controllers

Step 1 Choose Configuration > Template > Features & Technologies > Controller > WLANs > WLAN Configuration.

Step 2 Hover your mouse cursor over the tool tip next to the template type and click New.

Step 3 Complete the required fields in the General, Security, QoS, Advanced, HotSpot, Policy Mappings tabs, and then click Save as New Template.

Step 4 Proceed to deploy the template by click Deploy.

Related Topics
- Viewing Controller WLAN Configurations
- Adding Policies to Controller WLANs
- Configuring Mobile Concierge (802.11u) on WLANs
- Deleting Controller WLANs
- Scheduling Status Changes for Multiple Controller WLANs
- Viewing WLAN Mobility Anchors
Deleting Controller WLANs

**Step 1** Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

**Step 2** Click the Device Name of the appropriate controller.

**Step 3** From the left sidebar menu, choose WLANs > WLAN Configuration.

**Step 4** Select the check boxes of the WLANs that you want to delete.

**Step 5** Choose Select a command > Delete a WLAN > Go.

**Step 6** Click OK to confirm the deletion.

**Related Topics**
- Viewing Controller WLAN Configurations
- Adding Policies to Controller WLANs
- Configuring Mobile Concierge (802.11u) on WLANs
- Adding WLANs to Controllers
- Scheduling Status Changes for Multiple Controller WLANs
- Viewing WLAN Mobility Anchors

Scheduling Status Changes for Multiple Controller WLANs

Prime Infrastructure lets you change the status of more than one WLAN at a time on any given controller. You can select multiple WLANs and select the date and time for that status change to take place.

**Step 1** Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

**Step 2** Click the Device Name of the appropriate controller.

**Step 3** From the left sidebar menu, choose WLANs > WLAN Configuration.

**Step 4** Select the check boxes of the WLANs that you want to schedule for a status change.

**Step 5** From the Select a command drop-down list, choose Schedule Status to open the WLAN Schedule Task Detail page.

The selected WLANs are listed at the top of the page.

**Step 6** Enter a Scheduled Task Name to identify this status change schedule.

**Step 7** Choose the new Admin Status (Enabled or Disabled) from the drop-down list.

**Step 8** Choose the schedule time using the hours and minutes drop-down lists.

**Step 9** Click the calendar icon to choose a schedule date or enter the date in the text box (MM/DD/YYYY).

**Step 10** Select the appropriate Recurrence radio button to determine the frequency of the status change (Daily, Weekly, or No Recurrence).

**Step 11** Click Submit to initiate the status change schedule.
Mobility anchors are controllers defined as anchors for WLANs. Clients (that is, any 802.11 mobile station, such as a laptop) are always attached to one of the anchors.

You can use mobility anchors to restrict a WLAN to a single subnet, regardless of the client’s network entry point. Users can access a public or guest WLAN throughout the enterprise but will still be restricted to a specific subnet. You can also use guest WLANs to provide geographical load balancing, as WLANs can represent a particular section of a building (such as a lobby, restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller encapsulates the packets and forwards them to the client.

A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controllers can have a 4100 series controller or a 4400 series controller as its anchor.

The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

---

**Step 1** Choose **Configuration > Network > Network Devices**, then select **Device Type > Wireless Controller**.

**Step 2** Click the Device Name of the appropriate controller.

**Step 3** From the left sidebar menu, choose **WLANs > WLAN Configuration**.

**Step 4** Click a WLAN ID to view the parameters for a specific WLAN.

**Step 5** Click the **Advanced** tab.

**Step 6** Click the **Mobility Anchors** link. Prime Infrastructure displays the IP address and current status (for example, reachable) for each anchor.

---

**Related Topics**

- Viewing Controller WLAN Configurations
• Adding Policies to Controller WLANs
• Configuring Mobile Concierge (802.11u) on WLANs
• Adding WLANs to Controllers
• Deleting Controller WLANs
• Scheduling Status Changes for Multiple Controller WLANs

Configuring 802.11r Fast Transition

802.11r-enabled WLAN provides faster and better roaming experience for wireless client devices. However, legacy devices that do not recognize the fast transition (FT) authentication key-management (AKM) in robust secure network information exchange (in beacons and probe responses) cannot join the 802.11r-enabled WLAN.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller to view all the wireless controllers.

Step 2 Click Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose WLANs > WLAN Configuration to access the WLAN configuration page.

Step 4 Click WLAN ID to view the parameters for a specific WLAN.

Step 5 Click Security > Layer 2 tab.

Step 6 From the Layer 2 Security drop-down list, choose WPA+WPA2.

Step 7 Check or uncheck the Fast Transition check box to enable or disable Fast Transition. Fast Transition is enabled by default when you create a new WLAN, from Cisco WLC Release 8.3 onwards. However, the existing WLANs will retain the current configuration when Cisco WLC upgrades to Release 8.3 from an earlier release.

Step 8 Check or uncheck the Over the DS check box to enable or disable Fast Transition over a distributed system. This option is available only if you enable Fast Transition or if Fast Transition is adaptive.

Step 9 In the Reassociation Timeout text box, enter the number of seconds after which the reassociation attempt of a client to an AP should time out. The valid range is 1 to 100 seconds.

Note This option is available only if you enable Fast Transition.

Step 10 Under Authentication Key Management, choose FT 802.1X or FT PSK. Check or uncheck the corresponding check boxes to enable or disable the keys. If you check the FT PSK check box, from the PSK Format drop-down list, choose ASCII or HEX and enter the key value.

Note When Fast Transition adaptive is enabled, you can use only 802.1X and PSK.

Step 11 Click Save to save your settings.
Configuring Fastlane QoS

The Fastlane QoS feature provides better Quality of Service (QoS) treatment for Apple clients, when compared to other wireless clients. This feature is disabled by default.

**Note**

You should enable or disable this feature only during a maintenance window when not many clients are connected, as there will be a disruption in service when all the WLANs and the network are disabled and enabled again.

**Step 1** Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

**Step 2** Click Device Name of the appropriate controller.

**Step 3** From the left sidebar menu, choose WLANs > WLAN Configuration.

**Step 4** Click WLAN ID to view the parameters for a specific WLAN.

**Step 5** Click the QoS tab.

**Step 6** Check the Fastlane check box to enable Fastlane QoS.

**Step 7** Click Save to save your settings.

Disabling Fastlane QoS

**Note**

Fastlane must be disabled on all the WLANs before disabling Fastlane QoS.

**Step 1** Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

**Step 2** Click Device Name of the appropriate controller.

**Step 3** From the left sidebar menu, choose WLANs > WLAN Configuration.

**Step 4** From the Select a Command drop-down list, choose Disable Fastlane.

**Step 5** Click Save.

Working with WLAN AP Groups

Site-specific VLANs or AP (access point) groups allow you to segment WLANs into different broadcast domains. This allows you to minimize the total number of broadcast domains, which permits more effective load balancing and bandwidth allocation.

**Step 1** Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

**Step 2** Click Device Name of the appropriate controller.

**Step 3** From the left sidebar menu, choose WLAN > AP Groups. The AP groups summary page appears. This page displays a summary of the AP groups configured on the network.
From here you can add, remove, or view details of an AP group.

**Step 4** Click the AP group name on the Access Points tab to view or edit its access point(s).

**Step 5** Click the WLAN Profiles tab to view, edit, add, or delete WLAN profiles.

---

**Related Topics**

- Creating Controller WLAN AP Groups
- Deleting Controller WLAN AP Groups
- Deleting Controller WLAN AP Groups
- Configuring Controller WLANs
- Auditing Controller WLAN AP Groups

---

## Creating Controller WLAN AP Groups

Use the AP Groups detail page to add AP (access point) groups. Note that if the target controller is earlier than version 5.2, AP Groups are called AP Group VLANs.

**Step 1** Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

**Step 2** Click the Device Name of the appropriate controller.

**Step 3** From the left sidebar menu, choose WLAN > AP Groups.

**Step 4** Choose Select a command > Add AP Groups > Go. The AP Groups details page displays.

**Step 5** Create a new AP group, as follows:

a. Enter a name for the AP group.

b. Enter a description for the new AP group (this group description is optional).

**Step 6** Add access points to the new AP group, as follows:

a. Click the Access Points tab.

b. Click Add. The Access Point page displays a list of available access points.

c. Select the check boxes of the access points you want to add.

d. Click Select.

**Step 7** Add a WLAN profile, as follows:

a. Click the WLAN Profiles tab.

b. Click Add.

To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.

Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).
c. Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

d. Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.
   To display all available interfaces, delete the current interface in the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

e. Select the **NAC Override** check box, if applicable. NAC override is disabled by default.

f. Specify the policy configuration parameters by clicking the **Add/Edit** link.
   - **Policy Name**—Name of the policy.
   - **Policy Priority**—Configure policy priority between 1 and 16. No two policies can have same priority.

   Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

g. When access points and WLAN profiles are added, click **Save**.

**Step 8** (Optional): Add an RF profile, as follows:

a. Click the **RF Profiles** tab:

b. Complete the fields as follows:
   - 802.11a—Choose an RF profile for APs with 802.11a radios.
   - 802.11b—Choose an RF profile for APs with 802.11b radios.

**Step 9** Add Hyperlocation configuration parameters, as follows:

- Click the **Location Settings** tab and configure the following:
  - **Hyperlocation**—By enabling this option, all the APs associated to that controller which have the Hyperlocation module will be enabled.
  - **Packet Detection RSSI Minimum**—Adjust this value to filter out weak RSSI readings from location calculation.
  - **Scan Count Threshold for Idle Client Detection**—The maximum permissible count of the idle clients detected while scanning.
  - **NTP Server IP Address**—Enter the valid NTP server IP address. This IP address is used by all APs for time synchronization.

**Step 10** When you are finished adding APs, WLAN profiles, and RF profiles to the new AP Group, click **Save**.

Changing the WLAN-interface mapping in an AP Group removes the local VLAN mapping for FlexConnect APs in this group. These mappings need to be reconfigured after applying this change.

**Related Topics**

- Working with WLAN AP Groups
- Deleting Controller WLAN AP Groups
- Auditing Controller WLAN AP Groups
Deleting Controller WLAN AP Groups

Step 1  Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2  Click the Device Name of the appropriate controller.
Step 3  From the left sidebar menu, choose WLAN > AP Groups.
Step 4  Select the check box(es) of the AP Groups that you want to delete.
Step 5  Choose Select a command > Delete AP Groups > Go.
Step 6  Click OK to confirm the deletion.

Related Topics
- Working with WLAN AP Groups
- Creating Controller WLAN AP Groups
- Auditing Controller WLAN AP Groups

Auditing Controller WLAN AP Groups

It is possible for difference to occur between the values Prime Infrastructure has stored for an AP group and the actual values stored in the current controller and access points device configurations. Auditing the AP group will help you determine if this has occurred and resolve them.

Step 1  Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2  Click the Device Name of the appropriate controller.
Step 3  From the left sidebar menu, choose WLAN > AP Groups.
Step 4  Click the name of the access point group that you want to audit.
Step 5  Click Audit.

The Audit button is located at the bottom of the page, next to the Save and Cancel buttons.

Related Topics
- Working with WLAN AP Groups
- Creating Controller WLAN AP Groups
- Deleting Controller WLAN AP Groups

Configuring FlexConnect on APs

FlexConnect enables you to configure and control APs in a remote location from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect APs switch client data traffic and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.
The following figure illustrates a typical FlexConnect deployment.

**Figure 27-3 FlexConnect Deployment**

---

**Supported Platforms for FlexConnect**

FlexConnect is supported only on these components:

- 1130AG, 1240AG, 1142, and 1252 APs
- Cisco 2000, and 4400 series controllers,
- Catalyst 3750G Integrated Wireless LAN Controller Switch
- Cisco Wireless Services Module (WiSM)
- Controller Network Module for Integrated Services Routers

---
FlexConnect Guidelines and Limitations

Follow these guidelines when you configure FlexConnect:

- You can deploy FlexConnect with either a static IP address or a DHCP address. The DHCP server must be available locally and must be able to provide the IP address for the AP during bootup.
- The maximum transmission unit (MTU) must be at least 500 bytes.
- Round-trip latency must not exceed 300 milliseconds (ms) between the AP and the controller. If the 300 milliseconds round-trip latency cannot be achieved, configure the AP to perform local authentication.
- The controller can send multicast packets in the form of unicast or multicast packets to the AP. In FlexConnect mode, the AP can receive multicast packets only in unicast form.
- FlexConnect supports CCKM full authentication but not CCKM fast roaming.
- FlexConnect supports a 1-1 network address translation (NAT) configuration and port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option.
- VPN, IPsec, L2TP, PPTP, Fortress authentication, and Cranite authentication are supported for locally switched traffic if these security types are accessible locally at the AP.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- For FlexConnect APs, the interface mapping at the controller for WLANs configured for FlexConnect local switching is inherited at the AP as the default VLAN tagging. This can be easily changed per SSID and per FlexConnect AP. Non-FlexConnect APs tunnel all traffic back to the controller, and VLAN tagging is dictated by each interface mapping of the WLAN.
- VLAN is not enabled on the FlexConnect AP by default. When FlexConnect is enabled, the AP inherits the VLAN ID associated to the WLAN. This configuration is saved in the AP and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect AP in a VLAN-enabled domain. Otherwise, the AP cannot send and receive packets to and from the controller. When the client is assigned a VLAN from the RADIUS server, that VLAN is associated to the locally switched WLAN.

Related Topics
- FlexConnect Authentication Process

FlexConnect Authentication Process

A FlexConnect AP searches for a controller on booting up. The AP joins the controller, downloads the latest software image from the controller and configuration information, and initializes the radio. It saves the downloaded configuration in non-volatile memory for use in standalone mode.

A FlexConnect AP identifies the controller IP address in one of the following ways:

- If the AP has been assigned an IP address from a DHCP server, it discovers a controller through the regular CAPWAP discovery process [Layer 3 broadcast, over-the-air provisioning (OTAP), DNS, or DHCP option 43]. OTAP does not work when the AP is booting up for the first time.
- If the AP has been assigned a static IP address, it discovers a controller through any of the CAPWAP discovery process methods except DHCP option 43. If the AP is unable to discover a controller through Layer 3 broadcast or OTAP, we recommend DNS resolution. With DNS, any AP with a static IP address that knows of a DNS server can find at least one controller.
If you want the AP to discover a controller from a remote network where CAPWAP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the AP command-line interface) the controller to which the AP should connect.

**Related Topics**

- Supported Platforms for FlexConnect
- FlexConnect Guidelines and Limitations
- FlexConnect Operation Modes
- FlexConnect States

## FlexConnect Operation Modes

The two modes of operation for FlexConnect APs are:

- **Connected mode**—In this mode the FlexConnect AP has CAPWAP connectivity with the controller.
- **Standalone mode**—In this mode the controller is unreachable and the FlexConnect AP enters standalone mode and authenticates clients by itself.

When a FlexConnect AP enters standalone mode:

- All clients that are on centrally switched WLANs are disassociated.
- For 802.1X or web-authentication WLANs, existing clients are not disassociated, but the FlexConnect AP stops sending beacons when the number of associated clients reaches zero.
- Disassociation messages are sent to new clients associating to 802.1X or web-authentication WLANs.
- Controller-dependent activities such as 802.1X authentication, NAC, and web authentication (guest access) are disabled, and the AP does not send any Intrusion Detection System (IDS) reports to the controller.
- Radio Resource Management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements, use of the neighbor list, and rogue containment and detection) are disabled. However, a FlexConnect AP supports dynamic frequency selection in standalone modes.

The FlexConnect AP maintains client connectivity even after entering standalone mode. However, once the AP reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

The LEDs on the AP change as the device enters different FlexConnect modes.

**Related Topics**

- Supported Platforms for FlexConnect
- FlexConnect Guidelines and Limitations
- FlexConnect Authentication Process
- FlexConnect States
FlexConnect States

The FlexConnect WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- **Central authentication, central switching**—In this state, the controller handles client authentication, and all client data tunnels back to the controller. This state is valid only in connected mode.

- **Central authentication, local switching**—In this state, the controller handles client authentication, and the FlexConnect AP switches data packets locally. This state is supported only when the FlexConnect AP is in connected mode.

- **Local authentication, local switching**—In this state, the FlexConnect AP handles client authentication and switches client data packets locally. The authentication capabilities are present in the AP itself and thus reduces the latency requirements. Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode. This state is valid in standalone mode and connected mode.

Local authentication is useful when the following conditions cannot be met:

- A minimum bandwidth of 128 kbps.
- Round trip latency no greater than 100 ms.
- Maximum transmission unit (MTU) no smaller than 500 bytes.

Local authentication does not support:

- Guest Authentication.
- RRM information.
- Local radius.
- Roaming till the WLC and the other FlexConnect APs in the group are updated with the client information.

- **Authentication down, switching down**—In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses. This state is valid only in standalone mode.

- **Authentication down, local switching**—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

The WLANS enter the following states when a FlexConnect AP enters the standalone mode:

- Local authentication, local switching state if the WLANS are configured as open, shared, WPA-PSK, or WPA2-PSK authentication and continue new client authentications.

- Authentication down, switching down state if the WLANS configured to central switching.

- Authentication down, local switching state if the WLANS configured to local-switch.

Related Topics

- Supported Platforms for FlexConnect
- FlexConnect Guidelines and Limitations
- FlexConnect Authentication Process
- FlexConnect Operation Modes
- Configuring FlexConnect: Workflow
Configuring FlexConnect: Workflow

To configure FlexConnect, you must follow the instructions in this section in the following order:

1. Configuring the Switch at the Remote Site.
2. Configuring the Controller.
3. Configuring an AP for FlexConnect.
4. Connecting Client Devices to the WLANs.

Configuring the Switch at the Remote Site

To prepare the switch at the remote site, follow these steps:

Step 1  Connect the AP that is enabled for FlexConnect to a trunk or access port on the switch.
Step 2  Configure the switch to support the FlexConnect AP.

Related Topics

- Example: Configuring FlexConnect on Switches at Remote Sites
- Configuring the Controller for a Centrally Switched WLAN
- Configuring the Controller for a Locally Switched WLAN
- Configuring the Controller for a Centrally Switched WLAN for Guest Access

Example: Configuring FlexConnect on Switches at Remote Sites

In this sample configuration:

- The FlexConnect AP is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The AP needs IP connectivity on the native VLAN.
- The remote site has local servers/resources on VLAN 101.
- A DHCP pool is created in the local switch for both VLANs in the switch.
- The first DHCP pool (NATIVE) is used by the FlexConnect AP, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched.

The addresses in this sample configuration are for illustration purposes only. The addresses that you use must fit into your upstream network.

```bash
ip dhcp pool NATIVE
  network 10.10.100.0 255.255.255.0
  default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
  network 10.10.101.0 255.255.255.0
  default-router 10.10.101.1
!
interface FastEthernet1/0/1
  description Uplink port
  no switchport
  ip address 10.10.98.2 255.255.255.0
  spanning-tree portfast
```
Chapter 27      Configuring Wireless Devices

Configuring FlexConnect on APs

! interface FastEthernet1/0/2
description the Access Point port
switchport trunk encapsulation dot1q
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
spanning-tree portfast
!
interface Vlan100
ip address 10.10.100.1 255.255.255.0
ip helper-address 10.10.100.1
!
interface Vlan101
ip address 10.10.101.1 255.255.255.0
ip helper-address 10.10.101.1
end

Related Topics
- Configuring the Switch at the Remote Site
- Configuring the Controller for a Centrally Switched WLAN
- Configuring the Controller for a Locally Switched WLAN
- Configuring the Controller for a Centrally Switched WLAN for Guest Access

Configuring the Controller for a Centrally Switched WLAN

To create a centrally switched WLAN:

Step 1  Choose Configuration > Network > Network Devices > Wireless Controllers.
Step 2  Click the Device Name of the appropriate controller.
Step 3  From the left sidebar menu, choose WLAN > WLAN Configuration to access the WLAN Configuration page.
Step 4  Choose Add a WLAN from the Select a command drop-down list, and click Go.
Cisco APs can support up to 16 WLANs per controller. However, some Cisco APs do not support WLANs that have a WLAN ID greater than 8. In such cases when you attempt to create a WLAN the following message is displayed:

Not all types of AP support WLAN ID greater than 8, do you wish to continue?

Click OK to creates a WLAN with the next available WLAN ID.
If you have earlier deleted a WLAN that has a WLAN ID less than 8, then that ID is applied to the next created WLAN.

Step 5  Choose a template from the drop-down list to apply it to the controller.
To create a new WLAN template, click Click here link to be redirected to the template creation page.

Step 6  Choose WPA1+WPA2 from the Layer 2 Security drop-down list.

Step 7  Check the Status check box under General Policies to enable the WLAN.
If NAC is enabled and you have created a quarantined VLAN for use with this, make sure to select it from the Interface drop-down list under General Policies. Also, check the Allow AAA Override check box to ensure that the controller validates a quarantine VLAN assignment.
Step 8 Click Save.

Related Topics
- Configuring the Switch at the Remote Site
- Configuring the Controller for a Locally Switched WLAN
- Configuring the Controller for a Centrally Switched WLAN for Guest Access

Configuring the Controller for a Locally Switched WLAN

To create a locally switched WLAN:

Step 1 Create a new WLAN as described in Configuring the Controller for a Centrally Switched WLAN, Step 1 to Step 5.

Step 2 Click the WLAN ID and modify the configuration parameters.
Choose WPA1+WPA2 from the Layer 2 Security drop-down list. Make sure you choose PSK authentication key management and enter a preshared key.

Step 3 Check the Admin Status check box to this WLAN.

Step 4 Check the FlexConnect Local Switching check box to enable local switching.

Step 5 Click Save to commit your changes.

Related Topics
- Configuring the Switch at the Remote Site
- Configuring the Controller for a Centrally Switched WLAN
- Configuring the Controller for a Centrally Switched WLAN for Guest Access

Configuring the Controller for a Centrally Switched WLAN for Guest Access

To create a Centrally Switched WLAN for Guest Access to tunnel guest traffic to the controller:

Step 1 Create a new WLAN as described in Configuring the Controller for a Centrally Switched WLAN, Step 1 to Step 5.

Step 2 Click the WLAN to modify the following configuration parameters:
   b. Check the Web Policy check box.
   c. Select Authentication.
   d. Configure a preauthentication access control list (ACL) on the WLAN if you are using an external web server, and then choose this ACL as the WLAN preauthentication ACL.

Step 3 Check the Status check box under General Policies to enable the WLAN.
Step 4  Click **Save** to commit your changes.

**Related Topics**
- Configuring the Switch at the Remote Site
- Configuring the Controller for a Centrally Switched WLAN
- Configuring the Controller for a Locally Switched WLAN
- Adding Guest Users to a Centrally Switched WLAN for Guest Access
- Web Authentication Templates

**Adding Guest Users to a Centrally Switched WLAN for Guest Access**

To add a local user:

**Step 1**  Select **Configure > Controller Template Launch Pad**.
**Step 2**  Select **Security > Local Net Users** from the left sidebar menu.
**Step 3**  From the **Select a Command** drop-down list select **Add Template** click **Go**.
**Step 4**  Uncheck the **Import from File** check box.
**Step 5**  Enter a username and password for the local user.
**Step 6**  From the Profile drop-down list, choose the appropriate SSID.
**Step 7**  Enter a description of the guest user account.
**Step 8**  Click **Save**.

**Related Topics**
- Configuring the Controller for a Centrally Switched WLAN for Guest Access

**Configuring an AP for FlexConnect**

To configure an AP for FlexConnect, follow these steps:

**Step 1**  Add the AP physically to the network.
**Step 2**  Select **Configure > Access Points**.
**Step 3**  Select the AP from the AP Name list.
**Step 4**  Select **Configure > AP Configuration Templates > Lightweight AP** or **Autonomous AP** if the AP Mode field does not display FlexConnect.
   If the AP Mode field displays FlexConnect skip to Step 8.
**Step 5**  Select the AP from the AP Name list. The Lightweight AP Template Detail page appears.
**Step 6**  Check the **FlexConnect Mode supported** check box to view all the profile mappings.
   If you are changing the mode to FlexConnect and if the AP is not already in FlexConnect mode, all other FlexConnect parameters are not applied on the AP.
Chapter 27     Configuring Wireless Devices

Step 7 Check VLAN Support check box and enter the number of the native VLAN on the remote network in the Native VLAN ID text box.

Step 8 Click the Apply/Schedule tab to save your changes.

Step 9 Click the Edit link in the Locally Switched VLANs section to change the number of VLANs from which a client IP address is obtained.

Step 10 Click Save to save your changes.

Repeat this procedure for any additional APs that need to be configured for FlexConnect at the remote site.

Related Topics

- Configuring the Switch at the Remote Site
- Configuring the Controller for a Centrally Switched WLAN
- Configuring the Controller for a Locally Switched WLAN

Connecting Client Devices to the WLANs

Follow the instructions for your client device to create profiles that connect to the WLANs you created while configuring the controller.

In our example, you create three profiles on the client:

1. To connect to the centrally switched WLAN, create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. When the client becomes authenticated, it gets an IP address from the management VLAN of the controller.

2. To connect to the locally switched WLAN, create a client profile that uses WPA/WPA2 authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the local switch.

3. To connect to the centrally switched WLAN for Guest Access, create a profile that uses open authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the network local to the AP. After the client connects, the local user types any HTTP address in the web browser. You are automatically directed to the controller to complete the web-authentication process. When the web login page appears, enter the username and password.

To see if data traffic of the client is being locally or centrally switched, choose Monitor > Devices > Clients.

Related Topics

- Configuring the Switch at the Remote Site
- Configuring the Controller for a Centrally Switched WLAN
- Configuring the Controller for a Locally Switched WLAN
- Configuring the Controller for a Centrally Switched WLAN for Guest Access
FlexConnect AP Groups

FlexConnect enables you to configure and control APs in a remote location through a wide area network (WAN) link without deploying a controller in each location. There is no deployment restriction on the number of FlexConnect APs per location, but you can organize and group the APs.

By forming AP groups with similar configurations, a procedure such as CCKM fast roaming can be processed faster than going through the controller individually.

For example, to activate CCKM fast roaming, the FlexConnect APs must know the CCKM cache for all devices that could associate with it. If you have a controller with 300 APs and 1000 devices that can potentially connect, it is quicker and more practical to process and send the CCKM cache for the FlexConnect group rather than for all 1000 devices. One particular FlexConnect group could focus on a small number of APs so that devices in that group connect to and roam between those few APs. With the established group, features such as CCKM cache and backup RADIUS are configured for the entire FlexConnect group rather than being configured in each AP.

All of the FlexConnect APs in a group share the same WLAN, backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple FlexConnect APs in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a FlexConnect group rather than having to configure the same server on each AP.

The following figure illustrates a typical FlexConnect group deployment with a backup RADIUS server in the branch office.

Figure 27-4  FlexConnect Group Deployment

Related Topics
- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication
- Auditing FlexConnect Groups
FlexConnect Groups and Backup RADIUS Servers

You can configure the controller to allow a FlexConnect AP in standalone mode to perform full 802.1x authentication to a backup RADIUS server. You can either configure a primary RADIUS server or both a primary and secondary RADIUS server.

Related Topics
- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication
- Auditing FlexConnect Groups

FlexConnect Groups and CCKM

FlexConnect groups are required for CCKM fast roaming. When you configure your WLAN for CCKM fast secure roaming, EAP-enabled clients securely roam from one access point to another without the need to re-authenticate with the RADIUS server. Using CCKM, an access point uses a fast re-keying technique that enables Cisco client devices to roam from one access point to another typically in under 150 milliseconds. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications. The FlexConnect access points obtain the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller.

For example, if you have a controller with 300 APs and 100 clients that might associate, sending the CCKM cache for all 100 clients is not practical. If you create a FlexConnect group comprising a limited number of APs, the clients roam only among those four APs, and the CCKM cache is distributed among those four APs only when the clients associate to one of them.

CCKM fast roaming between FlexConnect and non-FlexConnect APs is not supported.

Related Topics
- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and Local Authentication
- Auditing FlexConnect Groups

FlexConnect Groups and Local Authentication

You can configure the controller to allow a FlexConnect AP in standalone mode to perform LEAP or EAP-FAST authentication for up to 20 statically configured users. The controller sends the static list of usernames and passwords to each FlexConnect AP when it joins the controller. Each AP in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous AP network to a lightweight FlexConnect AP network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous AP.

LEAP or EAP-FAST authentication can be used in conjunction with the FlexConnect backup RADIUS server. If a FlexConnect group is configured with both a backup RADIUS server and local authentication, the FlexConnect AP always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the FlexConnect AP itself (if the primary and secondary RADIUS servers are not reachable).
Related Topics

- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and CCKM
- Configuring FlexConnect AP Groups
- Auditing FlexConnect Groups

Viewing FlexConnect AP Groups

You can view a list of existing FlexConnect AP groups.

**Step 1** Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **FlexConnect > FlexConnect AP Groups**. The FlexConnect AP Groups page opens.

**Step 4** Click the group name to view details about the FlexConnect AP group.

Configuring FlexConnect AP Groups

To configure a FlexConnect AP group, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **FlexConnect > FlexConnect AP Groups**.

**Step 4** From the Select a command drop-down list, click **Add FlexConnect AP Group** to open the FlexConnect AP Group > Add From Template pane.

**Step 5** Choose a template from the Select a template to apply to this controller drop-down list.

**Step 6** Click **Apply**.

**Step 7** Configure the required FlexConnect AP Group parameters. You can add, edit, or remove any of the following mappings by clicking the required tab:

- VLAN-ACL Mapping—Valid VLAN ID range is 1-4094.
- WLAN-ACL Mapping—Select the FlexConnect access control list for external web authentication. You can add up to a maximum of 16 WebAuth ACLs.
- WebPolicy ACL—Select the FlexConnect access control list to be added as a web policy. You can add up to a maximum of 16 Web-Policy ACLs.
- Local Split
- Central DHCP
Default FlexConnect Group

- Central DHCP—When you enable this feature, the DHCP packets received from APs are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.

- Override DNS—You can enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.

- NAT-PAT—You can enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.

Step 8 To see if an individual access point belongs to a FlexConnect group, click the Users configured in the group link. The FlexConnect AP Group page shows the names of the groups and the access points that belong in it.

Step 9 Click Save.

Step 10 To delete an existing FlexConnect AP group, select the check box of the group you want to remove, and choose Delete FlexConnect AP Group from the Select a command drop-down list.

Related Topic
- Verifying APs in FlexConnect Groups

Verifying APs in FlexConnect Groups

To verify that an individual AP belongs to a FlexConnect group, click the Users configured in the group link. It takes you to the FlexConnect AP Group page, which shows the names of the groups and the APs that belong to it.

Related Topics
- Auditing FlexConnect Groups

Auditing FlexConnect Groups

If the FlexConnect configuration changes over a period of time either on Prime Infrastructure or the controller, you can audit the configuration. The changes are visible on subsequent screens. You can choose to synchronize the configuration by refreshing Prime Infrastructure or the controller.

Related Topics
- Configuring FlexConnect AP Groups
- Viewing FlexConnect AP Groups

Default FlexConnect Group

Default FlexConnect Group is a container where FlexConnect APs, which are not a part of any administrator-configured FlexConnect group, are added automatically when they associate with Cisco WLC.
Default FlexConnect group is created and stored when the controller comes up after an upgrade from an earlier release.

You cannot manually add or delete the default FlexConnect group. It is not possible to manually add or delete APs to the default FlexConnect group. The APs in the default FlexConnect group inherits the groups configuration. Any change to the group configuration is propagated to all the APs in the group.

When an administrator created group is deleted, all the APs from that group are moved to the default FlexConnect group and inherits the configuration of this group. Similarly, APs removed manually from other groups are also added to the default FlexConnect group.

When an AP from the default FlexConnect group is added to a customized group, the existing configuration (from Default FlexConnect Group) is deleted and the configuration from the customized group is pushed to the AP. If there is a standby controller, the default FlexConnect group and its configuration is also synchronized.

When an AP is converted from local mode to FlexConnect mode, and if it is not part of any administrator configured FlexConnect group, then it becomes a part of default FlexConnect group.

**Note**
Efficient AP Image Upgrade feature is not supported with the Default FlexConnect AP group.

**Related Topics**
- Moving APs from a Default FlexConnect Group to Another FlexConnect Group
- Delete FlexConnect AP Group

### Moving APs from a Default FlexConnect Group to Another FlexConnect Group

**Step 1** Choose **Configuration > Network > Network Devices**.

**Step 2** From the left pane, **Device Type > Wireless Controller**.

**Step 3** Click the name of the corresponding controller.

**Step 4** From the left pane, choose **FlexConnect > FlexConnect AP Groups**.

The FlexConnect AP Groups page appears.

**Step 5** Click a group name **Group Name link**.

**Step 6** From the FlexConnect AP Groups, click the **Group Name**.

**Step 7** In the FlexConnect AP tab, click **Add AP**. The Add FlexConnect AP page shows the APs from the default FlexConnect group.

**Step 8** Select any of the **AP Name** and click **Add**.

The selected AP will automatically added to the new group and gets deleted from the default FlexConnect group.

**Step 9** Click **Save**.

**Related Topics**
- Default FlexConnect Group
Delete FlexConnect AP Group

**Note**
You cannot delete the default FlexConnect group.

**Step 1**
Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2**
Click the device name of the applicable controller.

**Step 3**
From the left sidebar menu, choose **FlexConnect > FlexConnect AP Groups**.

**Step 4**
Click a Group Name and select **Delete FlexConnect AP Group** from the Select a Command drop-down list.

**Step 5**
Click OK to confirm the deletion.

**Related Topics**
- Default FlexConnect Group
- Configuring FlexConnect on APs

Configuring Controller Security Parameters

- Configuring Controller File Encryption
- Configuring Controllers AAA Security
- Local EAP on Controllers
- Configuring Controller Web Auth Certificates
- Configuring Controller User Login Policies
- Managing Manually Disabled Clients
- Configuring Controller Access Control Lists
- Configuring CPU Access Control Lists
- Configuring the IDS Sensor List
- Certificate Authority (CA) Certificates
- Identity Certificates
- Configuring Controller Web Auth Certificates
- Configuring Wireless Protection Policies
- Configuring Rogue Policies
- Configuring Rogue AP Rules
- Configuring Client Exclusion Policies
- Viewing Controller Standard Signature Parameters
- Configuring Custom Signatures
- Configuring AP Authentication and MFP
You can configure file encryption to ensure that data is encrypted when you upload or download controller configuration files from a TFTP server.

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > File Encryption.

**Step 4** Check the File Encryption box.

**Step 5** In the Encryption Key field, enter a text string of exactly 16 characters. Reenter the key in the Confirm Encryption Key field.

**Step 6** Click Save.

**Related Topics**
- Configuring Controller Security Parameters

**Configuring Controllers AAA Security**

This section describes how to configure controller security AAA parameters and contains the following topics:

- Configuring AAA General Parameters
- Viewing AAA RADIUS Auth Servers
- Viewing AAA RADIUS Acct Servers
- Configuring AAA RADIUS Fallback Parameters
- Configuring AAA LDAP Servers
- Configuring AAA TACACS+ Servers
- Viewing AAA Local Net Users
- Configuring AAA MAC Filtering
- Configuring AAA AP/MSE Authorization
- Configuring AAA Web Auth Configuration
- Configuring AAA Web Auth Configuration

**Configuring AAA General Parameters**

The General page allows you to configure the local database entries on a controller.

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Configuring Controller Security Parameters

Step 2  Click the device name of the applicable controller.
Step 3  From the left sidebar menu, choose Security > AAA > General - AAA.
Step 4  Enter the maximum number of allowed database entries. The valid range is 512 - 2048.
Step 5  In the Mgmt User Re-auth Interval, set the termination interval for management users.
Step 6  Reboot your server to apply the changes.

Related Topic
- Configuring Controllers AAA Security

Viewing AAA RADIUS Auth Servers

You can view a summary of existing RADIUS authentication servers

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2  Click the device name of the applicable controller.
Step 3  From the left sidebar menu, choose Security > AAA > RADIUS Auth Servers. The following RADIUS Auth Servers parameters appear:
  - Server Index—Access priority number for the RADIUS server (display only). Click to go to Configure IPaddr > RADIUS Authentication Server.
  - Server Address—IP address of the RADIUS server (read-only).
  - Port Number—Controller port number (read-only).
  - Admin Status—Enable or Disable.
  - Network User—Enable or Disable.
  - Management User—Enable or Disable.

Related Topics
- Configuring Controllers AAA Security
- Adding Authentication Servers

Adding Authentication Servers

To add an authentication server, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2  Click the device name of the applicable controller.
Step 3  From the left sidebar menu, choose Security > AAA > RADIUS Auth Servers.
Step 4  From the Select a command drop-down list, choose Add Auth Server to open the Radius Authentication Server > Add From Template page.
Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click Apply.

To create a new template for Radius authentication servers, choose Configuration > Templates > Features and Technologies > Controller > Security > AAA > RADIUS Auth Servers.

---

**Related Topic**
- Configuring Controllers AAA Security
- Viewing AAA RADIUS Auth Servers

---

**Viewing AAA RADIUS Acct Servers**

To view a summary of existing RADIUS accounting servers, follow these steps:

---

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers. RADIUS Acct Server parameters include the following:

- **Server Index**—Access priority number for the RADIUS server (read-only). Click to open the Radius Acct Servers Details page.
  
  To edit or audit the current accounting server parameters, click the Server Index for the applicable accounting server.

- **Server Address**—IP address of the RADIUS server (read-only).

- **Port Number**—Controller port number (read-only).

- **Admin Status**—Enable or Disable.

- **Network User**—Enable or Disable.

---

**Related Topic**
- Configuring Controllers AAA Security
- Adding an Accounting Server

---

**Adding an Accounting Server**

To add an accounting server, follow these steps:

---

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers.

**Step 4** From the Select a command drop-down list, choose Add Acct Server to open the Radius Acct Servers Details > Add From Template page.
Chapter 27      Configuring Wireless Devices

Configuring Controller Security Parameters

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 From the drop-down list, choose a controller on which to apply to this template.

Step 7 Click Apply.

To create a new template for Radius accounting servers, choose Configuration > Templates > Features and Technologies > Controller > Security > AAA > RADIUS Acct Servers.

Related Topic
- Configuring Controllers AAA Security
- Viewing AAA RADIUS Acct Servers

Deleting an Accounting Server

To delete an accounting server, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers.

Step 4 Select the check box(es) for the applicable accounting server(s).

Step 5 From the Select a command drop-down list, choose Delete Acct Server.

Step 6 Click Go.

Step 7 Click OK in the pop-up dialog box to confirm the deletion.

Related Topic
- Configuring Controllers AAA Security
- Viewing AAA RADIUS Acct Servers

Configuring AAA RADIUS Fallback Parameters

To configure RADIUS fallback parameters, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Fallback.

Step 4 Make the required changes, then click Save.

Step 5 Click Audit to check the present configuration status of Prime Infrastructure and the controller.
Related Topic
- Configuring Controllers AAA Security

Configuring AAA LDAP Servers

You can add and delete LDAP servers to controllers. Prime Infrastructure supports LDAP configuration for both an anonymous or authenticated bind.

To access the LDAP Servers page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > LDAP Servers.

This page displays LDAP servers currently used by this controller and contains the following parameters:
- Check box—Select the check box to choose an LDAP server for deletion.
- Server Index—A number assigned to identify the LDAP server. Click the index number to go the LDAP server configuration page.
- Server Address—The LDAP server IP address.
- Port Number—The port number used to communicate with the LDAP server.
- Admin Status—Server template status. Indicates if use of the LDAP server template is enabled or disabled.

Step 4 Click on a column title to toggle whether the information in sorted in ascending or descending order.

Related Topics
- Configuring New LDAP Bind Requests
- Configuring Controllers AAA Security

Adding LDAP Servers

To add an LDAP Server, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > LDAP Servers.

Step 4 From the Select a command drop-down list, choose Add LDAP Server.

Step 5 Click Go.
Related Topic
- Configuring Controllers AAA Security

Deleting LDAP Servers

To delete the LDAP Server, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Network &gt; Network Devices, then from the Device Groups menu on the left, select Device Type &gt; Wireless Controller.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the device name of the applicable controller.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose Security &gt; AAA &gt; LDAP Servers.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the check box(es) of the LDAP servers that you want to delete.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the Select a command drop-down list, choose Delete LDAP Servers.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Go.</td>
</tr>
</tbody>
</table>

Related Topic
- Configuring Controllers AAA Security

Configuring New LDAP Bind Requests

Prime Infrastructure supports LDAP configuration for both an anonymous or authenticated bind. A bind is a socket opening that performs a lookup.

To configure LDAP bind requests, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Network &gt; Network Devices, then from the Device Groups menu on the left, select Device Type &gt; Wireless Controller.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the device name of the applicable controller.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose Security &gt; AAA &gt; LDAP Servers.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click a value under the Server Index column.</td>
</tr>
<tr>
<td>Step 5</td>
<td>From the Bind Type drop-down list, choose Authenticated or Anonymous. If you choose Authenticated, you must enter a bind username and password as well.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.</td>
</tr>
<tr>
<td>Step 8</td>
<td>In the Server User Type text box, enter the ObjectType attribute that identifies the user.</td>
</tr>
<tr>
<td>Step 9</td>
<td>In the Retransmit Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Select the Admin Status check box if you want the LDAP server to have administrative privileges.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>
Related Topic

- Configuring Controllers AAA Security

### Configuring AAA TACACS+ Servers

You can add and delete TACACS+ servers to controllers. To access the TACACS+ Servers page, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > AAA > TACACS+ Servers.

This page displays TACACS+ servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose a TACACS+ server for deletion.
- Server Type—The TACACS+ server type—accounting, authorization, or authentication.
- Server Index—A number assigned to identify the TACACS+ server and set its use priority. Click the index number to go the TACACS+ server configuration page.
- Server Address—The TACACS+ server IP address.
- Port Number—The port number used to communicate with the TACACS+ server.
- Admin Status—Server template status. Indicates if use of the TACACS+ server template is enabled.

You can select one of the following options from the Select a command drop-down list:

- Add TACACS+ Server—Choose this option, then click Go to add a TACACS+ server to the controller.
- Delete TACACS+ Servers—Choose this option, then click Go to delete all TACACS+ servers with a selected check box from the controller.

**Step 4** Click on a column title to toggle whether the information in sorted in ascending or descending order.

Related Topic

- Configuring Controllers AAA Security

### Viewing AAA Local Net Users

You can view summary of the existing local network user controllers for clients who are allowed to access a specific WLAN. This is an administrative bypass of the RADIUS authentication process. Layer 3 Web Authentication must be enabled. The client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

To view existing local network users, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2  Click the device name of the applicable controller.
Step 3  From the left sidebar menu, choose **Security > AAA > Local Net Users**. The Local Net Users page displays the following local net user parameters:
- **Username**—User-defined identification.
- **WLAN ID**—Any WLAN ID, 1 through 16; 0 for all WLANs; 17 for third-party WLAN that this local net user is allowed to access.
- **Description**—Optional user-defined description.

**Related Topics**
- Deleting Local Net Users
- Configuring Controllers AAA Security

### Deleting Local Net Users

To delete a local net user, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.
**Step 2** Click the device name of the applicable controller.
**Step 3** From the left sidebar menu, choose **Security > AAA > Local Net Users**.
**Step 4** Select the check box(es) for the applicable local net user(s).
**Step 5** From the Select a command drop-down list, choose **Delete Local Net Users**.
**Step 6** Click **Go**.
**Step 7** Click **OK** in the dialog box to confirm the deletion.

**Related Topic**
- Configuring Controllers AAA Security

### Configuring AAA MAC Filtering

You can view MAC Filter information. You cannot use MAC address in the broadcast range.

**Step 1** Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.
**Step 2** Click the device name of the applicable controller.
**Step 3** From the left sidebar menu, choose **Security > AAA > MAC Filtering**. The MAC Filtering page displays the following parameters:
- **MAC Filter Parameters**
  - **RADIUS Compatibility Mode**—User-defined RADIUS server compatibility: Cisco ACS, FreeRADIUS, or Other.
MAC Delimiter—The MAC delimiters can be Colon (xx:xx:xx:xx:xx:xx), Hyphen (xx-xx-xx-xx-xx-xx), Single Hyphen (xxxxxx-xxxxxx), or No Delimiter (xxxxxxxxxxxx), as required by the RADIUS server.

- MAC Filters
  - MAC Address—Client MAC address. Click to open Configure IPaddr > MAC Filter.
  - WLAN ID—1 through 16, 17 = Third-party AP WLAN, or 0 = all WLANs.
  - Interface—Displays the associated Interface Name.
  - Description—Displays an optional user-defined description.

**Step 4** From the Select a command drop-down list, choose **Add MAC Filters** to add a MAC Filter, **Delete MAC Filters** to delete the template(s), or **Edit MAC Filter** Parameters to edit the MAC Filters.

**Step 5** Click **Go**.

**Related Topic**
- Configuring Controllers AAA Security

### Configuring AAA AP/MSE Authorization

The AP/MSE Authorization page displays the access point policies and the list of authorized access points along with the type of certificate that an access point uses for authorization.

You cannot use MAC address in the broadcast range.

To access the AP/MSE Authorization page, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **Security > AAA > AP or MSE Authorization**. The AP/MSE Authorization page displays the following parameters:

- **AP Policies**
  - Authorize APs—Enabled or Disabled.
  - Accept SSC-APs—Enabled or Disabled.

- **AP/MSE Authorization**
  - AP/MSE Base Radio MAC Address—The MAC address of the authorized access point. Click the AP/MSE Base Radio MAC Address to view AP/MSE Authorization details.
  - Type
  - Certificate Type—MIC or SSC.
  - Key Hash—The 40-hex long SHA1 key hash. The key hash is displayed only if the certificate type is SSC.

**Related Topics**
- Editing AP/MSE Policies
Configuring Controller Security Parameters

• Configuring Controllers AAA Security

Editing AP/MSE Policies

To edit AP/MSE Authorization access point policies, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > AP or MSE Authorization.

Step 4 From the Select a command drop-down list, select Edit AP Policies, then click Go.

Step 5 Edit the following parameters, if necessary:

• Authorize APs—Select the check box to enable access point authorization.

• Accept SSC-APs—Select the check box to enable the acceptance of SSE access points.

Step 6 Click Save to confirm the changes, Audit to perform an audit on these device values, or Cancel to close this page with no changes.

Related Topic

• Configuring Controllers AAA Security

Configuring AAA Web Auth Configuration

The Web Auth Configuration page enables the user to configure the web auth configuration type. If the type is configured as customized, the user downloaded web auth replaces the controller-provided internal web auth page.

To access the Web Auth Configuration page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > Web Auth Configuration.

Step 4 Select the Web Auth Type from the drop-down list.

Step 5 Configure the web auth parameters depending on the type chosen:

• Default Internal

  • Custom Redirect URL—URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.

  • Logo Display—Enable or disable logo display.

  • Web Auth Page Title—Title displayed on web authentication page.

  • Web Auth Page Message—Message displayed on web authentication page.

• Customized Web Auth
You can download an example login page and customizing the page. If you are using a customized web authentication page, it is necessary to download the example login.tar bundle file from the server, edit the login.html file and save it as either a .tar or .zip file, then download the .tar or .zip file to the controller.

Click the preview image to download this sample login page as a TAR. After editing the HTML you might click here to redirect to the Download Web Auth page. See the Downloading Customized WebAuthentication Bundles to Controllers for more information.

- **External**
  - External Redirect URL—Location of the login.html on an external server on the network.

If there are not any external web auth servers configured, you have the option of configuring one.

---

**Configuring AAA Password Policy**

This page enables you to determine your password policy.

To make modifications to an existing password policy, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > AAA > Password Policy.

**Step 4** Modify the password policy parameters as appropriate.

**Step 5** Click Save.

If you disable password policy options, you see a “Disabling the strong password check(s) will be a security risk as it allows weak passwords” message.

---

**Local EAP on Controllers**

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

When you enable local EAP, the controller serves as the authentication server and the local user database, making it independent of an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.
Configuring Local EAP General Parameters

You can specify a timeout value for local EAP. You can then add a template with this timeout value or make changes to an existing template.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then re-authenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

To specify a timeout value for local EAP, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **Security > Local EAP > General - Local EAP**.

**Step 4** Enter the Local Auth Active Timeout in the Local Auth Active Timeout text box (in seconds). Local Auth Active Timeout refers to the timeout period during which Local EAP is always used after all Radius servers are failed.

**Step 5** The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones.

You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. We recommend the default timeout on the Cisco ACS server of 20 seconds.

- Local EAP Identify Request Timeout =1 (in seconds)
- Local EAP Identity Request Maximum Retries=20 (in seconds)
- Local EAP Dynamic Wep Key Index=0
- Local EAP Request Timeout=20 (in seconds)
- Local EAP Request Maximum Retries=2
- EAPOL-Key Timeout=1000 (in milli-seconds)
- EAPOL-Key Max Retries=2
- Max-Login Ignore Identity Response

Roaming fails if these values are not set the same across multiple controllers.

**Step 6** Click **Save**.
Configuring Controller Security Parameters

Chapter 27      Configuring Wireless Devices

Related Topics
- Local EAP on Controllers
- Local EAP Profiles
- Configuring Local EAP General EAP-FAST Parameters
- Configuring Local EAP General Network Users Priority

Local EAP Profiles

You can apply a template for a local EAP profile or make modifications to an existing template. The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

Related Topics
- Viewing Existing Local EAP Profiles
- Adding Local EAP Profiles
- Local EAP on Controllers

Viewing Existing Local EAP Profiles

To view existing local EAP profiles, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Local EAP > Local EAP Profiles. The Local EAP Profiles page displays the following parameters:
- EAP Profile Name—User-defined identification.
- LEAP—Authentication type that leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- EAP-FAST—Authentication type (Flexible Authentication via Secure Tunneling) that uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- TLS—Authentication type that uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- PEAP—Protected Extensible Authentication Protocol.

Related Topics
- Local EAP on Controllers
- Local EAP Profiles
Adding Local EAP Profiles

To add a local EAP profile, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > Local EAP > Local EAP Profile.

**Step 4** From the Select a command drop-down list, choose Add Local EAP Profile.

**Step 5** Choose a template from the Select a template to apply to this controller drop-down list.

**Step 6** Click Apply.

**Related Topics**
- Local EAP on Controllers
- Local EAP Profiles
- Configuring Local EAP General Parameters
- Configuring Local EAP General EAP-FAST Parameters
- Configuring Local EAP General Network Users Priority

Configuring Local EAP General EAP-FAST Parameters

The EAP-FAST authentication type (Flexible Authentication via Secure Tunneling) uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC are used to perform mutual authentication with the RADIUS server through the access point.

To set EAP-FAST Parameters, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > Local EAP > EAP-FAST Parameters.

**Step 4** Enter the following parameters:
- Time to live for the PAC—The number of days for the PAC to remain viable. The valid range is 1 to 1000 days; the default setting is ten days.
- Authority ID—the authority identifier of the local EAP-FAST server in hexadecimal characters. You can enter up to 32 hexadecimal characters but it must be an even number of characters.
- Authority Info—the authority identifier of the local EAP-FAST server in text format.
- Server Key—the key (in hexadecimal characters) used to encrypt and decrypt PACs.
- Confirm Server Key—Verify the correct Server Key by re-typing it.
Anonymous Provision—Select the check box to enable anonymous provisioning. This feature allows PACs to be sent automatically to clients that do not have one during PAC provisioning. If this feature is disabled, PACs must be manually provisioned.

Step 5 Click Save.

Related Topics
- Local EAP on Controllers
- Local EAP Profiles
- Configuring Local EAP General Parameters
- Local EAP Profiles
- Configuring Local EAP General Network Users Priority

Configuring Local EAP General Network Users Priority

To specify the order that LDAP and local databases use to retrieve user credential information, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 From the left sidebar menu, choose Security > Local EAP > Network Users Priority.
Step 4 Use the left and right pointing arrows to include or exclude network credentials in the right-most list.
Step 5 Use the up and down buttons to determine the order credentials are attempted.
Step 6 Click Save.

Related Topics
- Local EAP on Controllers
- Local EAP Profiles
- Certificate Authority (CA) Certificates
- Configuring Controller Web Auth Certificates

Configuring Controller Web Auth Certificates

You can download a web authorization certificate or regenerate the internally-generated web auth certificate.

❗ Caution Each certificate has a variable-length embedded RSA Key. The RSA key can vary from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 Bits.
Chapter 27  Configuring Wireless Devices

Configuring Controller Security Parameters

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Web Auth Certificate.

Step 4 Click Download Web Auth Certificate to access the Download Web Auth Certificate to Controller page.

Related Topics
- Local EAP on Controllers
- Configuring Local EAP General Parameters
- Local EAP Profiles
- Configuring Local EAP General EAP-FAST Parameters

Configuring Controller User Login Policies

To configure the user login policies for controllers, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > User Login Policies.

Step 4 Enter the maximum number of concurrent logins allowed for a single username.

Step 5 Click Save.

Managing Manually Disabled Clients

The Disabled Clients page enables you to view excluded (blacklisted) client information. Clients who fail to authenticate three times when attempting to associate are automatically blocked, or excluded, from further association attempts for an operator-defined timeout. After the Excluded timeout, the client is allowed to retry authentication until it associates or fails authentication and is excluded again.

You cannot use MAC address in the broadcast range.

To access the Manually Disabled Clients page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Manually Disabled Clients. The Manually Disabled Clients page displays the following parameters:
Configuring Controller Security Parameters

- MAC Address—Disabled Client MAC addresses. Click a list item to edit the disabled client description.
- Description—Optional description of disabled client.

Configuring Controller Access Control Lists

You can view, edit, or add a new access control list (ACLs) for controllers.

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > Access Control Lists.

- Check box—Use the check box to select one or more ACLs for deletion.
- ACL Name—User-defined name of this template. Click an ACL item to view its parameters.

Related Topic
- Configuring Access Control List Rules
- Configuring CPU Access Control Lists

Configuring Access Control List Rules

You can create and modify access control list Access Control Lists (ACL) rules applied to controllers.

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > Access Control Lists.

**Step 4** Click an ACL name.

- Check box—Select to delete access control list rules.
- Seq#—You can define up to 64 Rules for each ACL. The Rules for each ACL are listed in contiguous sequence from 1 to 64. That is, if Rules 1 through 4 are already defined and you add Rule 29, it is added as Rule 5.

  If you add or change a Sequence number, Prime Infrastructure adjusts the other rule sequence numbers to retain the contiguous sequence. For instance, if you have Sequence numbers 1 through 7 defined and change number 7 to 5, operating system automatically reassigns Sequence 6 to 7 and Sequence 5 to 6.

- Action—Permit, Deny.
- Source IP/Mask—Source IP address and mask.
- Destination IP/Mask—Destination IP address and mask.
- Protocol—Protocol to use for this ACL:
Configuring Controller Security Parameters

- Any—All protocols
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol
- ICMP—Internet Control Message Protocol
- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP—Internet Protocol
- Eth Over IP—Ethernet over Internet Protocol
- Other Port OSPF—Open Shortest Path First
- Other—Any other IANA protocol (http://www.iana.org/)

If TCP or UDP is selected, Source Port and Dest Port parameters appear:

- Source Port—Source Port. Can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS SS, MS Dir Server, Other and Port Range.
- Dest Port—Destination port. If TCP or UDP is selected, can be Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS SS, MS Dir Server, Other and Port Range.

- DSCP (Differentiated Services Code Point)—Any, or 0 through 255.

### Adding New ACL Rules

**Step 1** Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **Security > Access Control Lists**.

**Step 4** Click an ACL name.

**Step 5** Click an applicable Seq#, or choose **Add New Rule** to access this page.

**Related Topics**

- Configuring Controller Access Control Lists
- Configuring CPU Access Control Lists
FlexConnect Access Control Lists

The ACLs on FlexConnect provide a mechanism to cater to the need for access control at the FlexConnect access point for protection and integrity of locally switched data traffic from the access point.

Related Topics
- Adding FlexConnect Access Control Lists
- Deleting FlexConnect Access Control Lists

Adding FlexConnect Access Control Lists

To add an Access Control List for FlexConnect access points, follow these steps:

---

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 From the left sidebar menu, choose Security > FlexConnect ACLs.
Step 4 From the Select a command drop-down list, choose Add FlexConnect ACLs.
Step 5 Click Go.

You cannot add a FlexConnect ACL if there is no template created. If you try to create an FlexConnect ACL when there are no templates available, you are redirected to the New Controller Templates page where you can create a template for FlexConnect ACL.

Step 6 Choose a template from the drop-down list to apply to the controller, and click Apply.

The FlexConnect ACL that you created appears in Configure > Controllers > IP Address > Security > FlexConnect ACLs.

---

Related Topics
- FlexConnect Access Control Lists

Deleting FlexConnect Access Control Lists

To delete a FlexConnect ACL, follow these steps:

---

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 From the left sidebar menu, choose Security > FlexConnect ACLs.
Step 4 From the FlexConnect ACLs page, select one or more FlexConnect ACLs to delete.
Step 5 From the Select a command drop-down list, choose Delete FlexConnect ACLs.
Step 6 Click Go.
Configuring CPU Access Control Lists

Access control lists (ACLs) can be applied to the controller CPU to control traffic to the CPU.

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > CPU Access Control Lists.

**Step 4** Select the Enable CPU ACL check box to enable the CPU ACL. The following parameters are available:
- ACL Name—Choose the ACL to use from the ACL Name drop-down list.
- CPU ACL Mode—Choose which data traffic direction this CPU ACL list controls.

Related Topics
- FlexConnect Access Control Lists
- Configuring Controller Access Control Lists
- Configuring Access Control List Rules

Configuring the IDS Sensor List

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS (Intrusion Detection System) sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > IDS Sensor Lists.

The IDS Sensor page lists all IDS sensors that have been configured for this controller. Click an IP address to view details for a specific IDS sensor.

Certificate Authority (CA) Certificates

A Certificate Authority (CA) certificate is a digital certificate issued by one certificate authority (CA) for another certification CA.

Related Topics
- Importing CA Certificates
Configuring Controller Security Parameters

Pasting CA Certificates Directly

Importing CA Certificates

To import a CA certificate from a file, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 From the left sidebar menu, choose Security > IP Sec Certificates > CA Certificate.
Step 4 Click Browse to navigate to the applicable certificate file.
Step 5 Click Open, then click Save.

Related Topics
- Certificate Authority (CA) Certificates

Pasting CA Certificates Directly

To paste a CA certificate directly, follow these steps:

Step 1 Copy the CA certificate to your computer clipboard.
Step 2 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 3 Click the device name of the applicable controller.
Step 4 From the left sidebar menu, choose Security > IP Sec Certificates > CA Certificate.
Step 5 Select the Paste check box.
Step 6 Paste the certificate directly into the text box.
Step 7 Click Save.

Related Topics
- Certificate Authority (CA) Certificates
- Identity Certificates
- Configuring Controller Web Auth Certificates

Identity Certificates

This page lists the existing network Identity (ID) certificates by certificate name. An ID certificate can be used by web server operators to ensure secure server operation. ID certificates are available only if the controller is running Cisco Unified Wireless Network Software Version 3.2 or higher.

- Importing ID Certificates
- Pasting ID Certificates
Importing ID Certificates

To import an ID certificate from a file, follow these steps:

Step 1: Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2: Click the device name of the applicable controller.

Step 3: From the left sidebar menu, choose Security > IP Sec Certificates > ID Certificate.

Step 4: From the Select a command drop-down list, choose Add Certificate.

Step 5: Click Go.

Step 6: Enter the Name and Password.

Step 7: Click Browse to navigate to the applicable certificate file.

Step 8: Click Open, then click Save.

Related Topics
- Identity Certificates

Pasting ID Certificates

To paste an ID certificate directly, follow these steps:

Step 1: Copy the ID certificate to your computer clipboard.

Step 2: Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 3: Click the device name of the applicable controller.

Step 4: From the left sidebar menu, choose Security > IP Sec Certificates > ID Certificate.

Step 5: From the Select a command drop-down list, choose Add Certificate.

Step 6: Click Go.

Step 7: Enter the Name and Password.

Step 8: Select the Paste check box.

Step 9: Paste the certificate directly into the text box.

Step 10: Click Save.

Related Topics
- Identity Certificates
- Certificate Authority (CA) Certificates
- Identity Certificates
Configuring Wireless Protection Policies

This section describes the wireless protection policy configurations and contains the following topics:

- Configuring Rogue Policies
- Configuring Rogue AP Rules
- Configuring Client Exclusion Policies
- Viewing Controller Standard Signature Parameters
- Configuring Custom Signatures
- Configuring AP Authentication and MFP

Configuring Rogue Policies

You can set up policies for rogue access points. Make sure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all access points joined to a controller (except for OfficeExtend access points). However, in Prime Infrastructure software Release 6.0 or later, you can enable or disable rogue detection for individual access points by selecting or unselecting the Rogue Detection check box in the Access Point Details page.

Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

To access the Rogue Policies page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > Rogue Policies. The following parameters appear:

- Rogue Location Discovery Protocol—RLDP determines whether or not the rogue is connected to the enterprise wired network. Choose one of the following from the drop-down list:
  - Disable—Disables RLDP on all access points. This is the default value.
  - All APs—Enables RLDP on all access points.
  - Monitor Mode APs—Enables RLDP only on access points in monitor mode.

- Rogue APs
  - Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)—Enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds and the default value is 1200 seconds.
    If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.
  - Rogue Detection Report Interval—Enter the time interval in seconds at which the APs should send the rogue detection report to the controller. Valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
  - Rogue Detection Minimum RSSI—Enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. Valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.
There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

- Rogue Detection Transient Interval—Enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

- Rogue Clients
  - Validate rogue clients against AAA—Select the check box to use the AAA server or local database to validate if rogue clients are valid clients. The default value is unselected.
  - Detect and report Adhoc networks—Select the check box to enable ad-hoc rogue detection and reporting. The default value is selected.

**Related Topics**
- Configuring Wireless Protection Policies
- Configuring Rogue AP Rules
- Configuring Client Exclusion Policies
- Viewing Controller Standard Signature Parameters
- Configuring Custom Signatures
- Configuring AP Authentication and MFP

**Configuring Rogue AP Rules**

This page enables you to view and edit current Rogue AP Rules.

To access the Rogue AP Rules page, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > Wireless Protection Policies > Rogue AP Rules. The Rogue AP Rules displays the Rogue AP Rules, the rule types (Malicious or Friendly), and the rule sequence.

**Step 4** Click a Rogue AP Rule to view or edit its details.

**Related Topics**
- Configuring Wireless Protection Policies
- Configuring Rogue Policies
- Configuring Client Exclusion Policies
- Viewing Controller Standard Signature Parameters
Chapter 27  Configuring Wireless Devices

Configuring Controller Security Parameters

Configuring Custom Signatures
Configuring AP Authentication and MFP

Configuring Client Exclusion Policies

This page enables you to set, enable, or disable the client exclusion policies applied to the controller.

To access the Client Exclusion Policies page, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose Security > Wireless Protection Policies > Client Exclusion Policies. The following parameters appear:

- Excessive 802.11a Association Failures—If enabled, clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- Excessive 802.11a Authentication Failures—If enabled, clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- Excessive 802.11x Authentication Failures—If enabled, clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- Excessive 802.11 Web Authentication Failures—If enabled, clients are excluded on the fourth web authentication attempt, after three consecutive failures.
- IP Theft Or Reuse—If enabled, clients are excluded if the IP address is already assigned to another device.

**Step 4** Click Save to save the changes made to the client exclusion policies and return to the previous page or click Audit to compare Prime Infrastructure values with those used on the controller.

Related Topics

- Configuring Wireless Protection Policies
- Configuring Rogue Policies
- Configuring Rogue AP Rules
- Configuring IDS Signatures
- Viewing Controller Standard Signature Parameters
- Configuring Custom Signatures
- Configuring AP Authentication and MFP

Configuring IDS Signatures

You can configure IDS Signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.
Cisco supports 17 standard signatures on controllers.

**Related Topics**
- Viewing Controller Standard Signature Parameters
- Configuring Custom Signatures
- Configuring AP Authentication and MFP

### Viewing Controller Standard Signature Parameters

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller.

To access the Standard Signatures page, follow these steps:

**Step 1**
Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2**
Click the device name of the applicable controller.

**Step 3**
From the left sidebar menu, choose **Security > Wireless Protection Policies > Standard Signatures**.
This page displays the following parameters:
- **Precedence**—The order in which the controller performs the signature checks.
- **Name**—The type of attack the signature is trying to detect.
- **Frame Type**—Management or data frame type on which the signature is looking for a security attack.
- **Action**—What the controller is directed to do when the signature detects an attack. For example:
  - **None**—No action is taken.
  - **Report**—Report the detection.
- **State**—Enabled or Disabled.
- **Description**—A more detailed description of the type of attack the signature is trying to detect.

**Step 4**
Click a signature Name to view individual parameters and to enable or disable the signature.

**Related Topics**
- Configuring IDS Signatures
- Uploading Signature Files
- Global Settings for Standard and Custom Signatures

### Downloading Signature Files

To download a signature file, follow these steps:

**Step 1**
Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2**
Click the device name of the applicable controller.

Step 4 From the Select a command drop-down list, choose Download Signature Files.

Step 5 Click Go.

Step 6 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 7 Choose Local Machine from the File is Located On. If you know the filename and path relative to the server root directory, you can also choose TFTP server.

Step 8 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries.

Step 9 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout.

Step 10 The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click Browse to navigate to it. A “revision” line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

If the transfer times out for some reason, choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to Prime Infrastructure own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in Prime Infrastructure server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 Click OK.

Related Topics
- Configuring IDS Signatures

Uploading Signature Files

You can upload a signature file from controllers. Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port cannot be routed.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port cannot be routed.
- A third-party TFTP server cannot run on the same computer as Prime Infrastructure because Prime Infrastructure built-in TFTP server and third-party TFTP server use the same communication port:

Step 1 Obtain a signature file from Cisco (standard signature file).

Step 2 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 3 Click the device name of the applicable controller.

Step 5 From the Select a command drop-down list, choose **Upload Signature Files from controller**.

Step 6 Specify the TFTP server name being used for the transfer.

Step 7 If the TFTP server is new, enter the TFTP IP address in the **Server IP Address** field.

Step 8 Choose **Signature Files** from the File Type drop-down list.

   The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File field (this field only shows if the Server Name is the default server). The controller uses this local filename as a base name and then adds _std.sig as a suffix for standard signature files and _custom.sig as a suffix for custom signature files.

Step 9 Click **OK**.

---

**Related Topics**

- [Downloading Signature Files](#)
- [Configuring IDS Signatures](#)

**Global Settings for Standard and Custom Signatures**

This command enables all signatures that were individually selected as enabled. If this text box remains unselected, all files are disabled, even those that were previously enabled. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

To enable all standard and custom signatures currently on the controller, follow these steps:

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the Select a command drop-down list, choose **Edit Signature Parameters**.

Step 4 Click **Go**.

Step 5 Select the **Enable Check for All Standard and Custom Signatures** check box.

Step 6 Click **Save**.

---

**Related Topic**

- [Configuring IDS Signatures](#)

**Enabling or Disabling Individual Signatures**

Step 1 Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

Step 2 Click the device name of the applicable controller.

Step 3 From the Select a command drop-down list, choose **Edit Signature Parameters**.

Step 4 Click an applicable Name for the type of attack you want to enable or disable.
The Standard Signature parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following parameters are displayed in both the signature page and the detailed signature page:

- **Precedence**—The order, or precedence, in which the controller performs the signature checks.
- **Name**—The type of attack the signature is trying to detect.
- **Description**—A more detailed description of the type of attack that the signature is trying to detect.
- **Frame Type**—Management or data frame type on which the signature is looking for a security attack.
- **Action**—What the controller is directed to do when the signature detects an attack. One possibility is *None*, where no action is taken, and another is *Report*, to report the detection.
- **Frequency**—The signature frequency or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 50 packets per interval.
- **Quiet Time**—The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds and the default value is 300 seconds.
- **MAC Information**—Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
- **MAC Frequency**—The signature MAC frequency or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 30 packets per interval.
- **Interval**—Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds and the default value is 1 second.
- **Enable**—Select this check box to enable this signature to detect security attacks or unselect it to disable this signature.
- **Signature Patterns**—The pattern that is being used to detect a security attack.

**Step 5**
From the Enable drop-down list, choose *Yes*. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.

**Step 6**
Click *Save*.

**Related Topics**
- Configuring IDS Signatures
- Configuring Rogue Policies
- Configuring Rogue AP Rules
- Configuring IDS Signatures
- Configuring Custom Signatures
- Configuring AP Authentication and MFP
Configuring Custom Signatures

The Custom Signature page shows the list of customer-supplied signatures that are currently on the controller.

Step 1
Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2
Click the device name of the applicable controller.

Step 3
From the left sidebar menu, choose Security > Wireless Protection Policies > Custom Signatures. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Step 4
Click a signature Name to view individual parameters and to enable or disable the signature.

Related Topics
- Configuring IDS Signatures
- Downloading Signature Files
- Uploading Signature Files
- Global Settings for Standard and Custom Signatures
- Configuring IDS Signatures
- Viewing Controller Standard Signature Parameters
- Configuring AP Authentication and MFP

Configuring AP Authentication and MFP

You can set the access point authentication policy and MFP (Management Frame Protection).

Step 1
Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2
Click the device name of the applicable controller.

Step 3
From the left sidebar menu, choose Security > Wireless Protection Policies > AP Authentication and MFP. This page displays the following fields:
• RF Network Name—Not an editable text box. The RF Network Name entered in the General parameters page is displayed here.

• Protection Type—From the drop-down list, choose one of the following authentication policies:
  – None—No access point authentication policy.
  – AP Authentication—Apply authentication policy.
  – MFP—Apply Management Frame Protection.

• Alarm Trigger Threshold—(Appears only when AP Authentication is selected as the Protection Type). Set the number of hits to be ignored from an alien access point before raising an alarm. The valid range is from 1 to 255. The default value is 255.

**Related Topics**

• Configuring Rogue Policies
• Configuring Rogue AP Rules
• Configuring IDS Signatures
• Viewing Controller Standard Signature Parameters
• Configuring Custom Signatures

### Configuring URL ACL Filtering

The feature allows network administrator to define HTTP URLs based Access Control Lists (ACL) in order to allow or disallow traffic.

The URL filtering feature helps optimize network bandwidth utilization by restricting access to websites. This feature gives you control to build URL ACLs, using which you can either permit or deny access to websites. These ACLs can be applied to locations, AP groups, WLAN profiles, and trusted and nontrusted clients within the same SSID.

Cisco WLC supports up to 64 ACLs and each ACL contains up to 100 URLs. These ACLs are configured to allow or deny requests and are associated with different interfaces, which helps in effective filtering.

The number of rules supported in each ACL varies for controllers:

• Cisco 5508 WLC and Cisco WiSM2 supports 64 rules in an ACL.
• Cisco 5520 WLC, Cisco 8510 WLC, and Cisco 8540 WLC supports 100 rules in an ACL.

**Restrictions for URL Filtering**

• Not supported on Cisco 2504 WLC, Cisco vWLC, and Cisco Mobility Express.
• Not supported in Flex mode with local switching.
• Supported on WLAN central switching and not on local switching.
• URL name is limited to 32 characters.
• HTTPS URLs are not supported.
• ACL may fail to filter in the following situations:
  – URL is across fragmented packets.
  – IP packets are fragmented.
Direct IP address or proxy setup is used instead URL.

- If any URL matches with these conditions, it will not be considered for filtering:
  - Wildcard URLs (ex: www.uresour*loc.com)
  - Sub-URL (ex: www.uresour*loc.com/support)
  - Sub-Domain (ex: reach.url.com or sub1.url.com)

### Configuring Access Control Lists

**Step 1** Choose **Configuration > Network > Network Devices**.

**Step 2** From the left pane, choose **Device Type > Wireless Controller**.

**Step 3** Click the name of the corresponding controller.

**Step 4** From the left pane, choose **Security > URL ACLs** to open the URL ACLs page.

**Step 5** Click the name of the URL ACL.

**Step 6** Under **Rules**, click **Add Row** to add a new ACL.

  - Specify a name for the new URL ACL.
  - From the **Rule Action** drop-down list, select **Allow** or **Deny**.

**Step 7** Click **Save**.

**Related Topics**

- Configuring Controller Security Parameters
- Deleting an URL ACL

### Deleting an URL ACL

**Step 1** Choose **Configuration > Network > Network Devices > Controllers**.

**Step 2** From the left pane, choose **Device Type > Wireless Controller**.

**Step 3** Click the name of the corresponding controller.

**Step 4** From the left pane, choose **Security > URL ACLs**.

**Step 5** Check the check boxes of the URL ACLs that you want to delete.

**Step 6** From the **Select a command** drop-down list, choose **Delete URL ACLs**.

**Step 7** Click **Go**.

**Note** If you want to clear the counters for an ACL, from the **Select a command** drop-down list, choose **Clear Counters**.

**Related Topics**

- Configuring Controller Security Parameters
802.11 Parameters

- Configuring General Parameters for 802.11 Controllers
- Configuring Aggressive Load Balancing
- Configuring Band Selection
- Configuring 802.11 Media Parameters
- Configuring RF Profiles (802.11)

Configuring General Parameters for 802.11 Controllers

You can edit country selection and timer information on a 802.11 controllers. To access this page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 Choose 802.11 > General - 802.11 from the left sidebar menu. The page opens and displays the following parameters:

- Country
  - Country—Countries and the protocols allowed. The maximum number of countries that you can select is 20.
  - Selected Countries—Displays countries currently selected.
- Timers
  - Authentication Response Timeout—Configures 802.11 authentication response timeout in seconds.

Related Topics

- Setting Multiple Country Codes
- Configuring Aggressive Load Balancing
- Configuring Band Selection
- Configuring 802.11 Media Parameters
- Configuring RF Profiles (802.11)

Setting Multiple Country Codes

To set multiple country support for a single controller that is not part of a mobility group, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 Choose 802.11 > General from the left sidebar menu.
Chapter 27 Configuring Wireless Devices

Configuring Controller Security Parameters

Step 4 Select the check box to choose which country you want to add. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country regulations.

Access points might not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase access points that match your country regulatory domain. For a complete list of country codes supported per product, see the following URL:

Step 5 Enter the time (in seconds) after which the authentication response times out.

Step 6 Click Save.

Related Topics
- Configuring General Parameters for 802.11 Controllers
- Configuring Aggressive Load Balancing
- Configuring Band Selection
- Configuring 802.11 Media Parameters
- Configuring RF Profiles (802.11)

Configuring Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance the wireless clients across access points. Clients are load balanced between the access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. This code indicates whether the access point can accept any more associations. If the access point is too busy, the client attempts to associate to a different access point in the area. The system determines if an access point is relatively more busy than its neighbor access points that are also accessible to the client.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it is allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

To configure aggressive load balancing, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose 802.11 > Load Balancing from the left sidebar menu. The Load Balancing page appears.
**Step 4** Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

\[
\text{load-balancing page + client associations on AP with lightest load} = \text{load-balancing threshold}
\]

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

**Step 5** Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

**Step 6** Click **Save**.

**Step 7** To enable or disable aggressive load balancing on specific WLANs, browse to the WLAN Configuration page, and click the **Advanced** tab. For instructions on using the WLAN Configuration page, see Configuring Controller WLANs in Related Topics.

---

**Related Topics**

- Configuring General Parameters for 802.11 Controllers
- Configuring Aggressive Load Balancing
- Configuring Band Selection
- Configuring 802.11 Media Parameters
- Configuring RF Profiles (802.11)
- Configuring Controller WLANs

---

**Configuring Band Selection**

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three non-overlapping channels. To combat these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

You can enable band selection globally on a controller, or you can enable or disable band selection for a particular WLAN, which is useful if you want to disable it for a select group of clients (such as time-sensitive voice clients).

Band-selection-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

**Guidelines for Using Band Selection**

Follow these guidelines when using band selection:

- Band selection can be used only with Cisco Aironet 1140 and 1250 series access points.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

Configuration Steps
To configure band selection, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** Choose 802.11 > Band Select from the left sidebar menu. The Band Select page appears.

**Step 4** Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

**Step 5** Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

**Step 6** Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

**Step 7** Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

**Step 8** Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

**Step 9** Click Save.

**Step 10** To enable or disable band selection on specific WLANs, browse to the WLAN Configuration page and click the Advanced tab. For instructions on using the WLAN Configuration page, see Configuring Controller WLANs in Related Topics.

Related Topics
- Configuring General Parameters for 802.11 Controllers
- Configuring Aggressive Load Balancing
- Configuring 802.11 Media Parameters
- Configuring RF Profiles (802.11)
- Configuring Controller WLANs

Configuring Preferred Call

The Preferred Call feature enables you to specify highest priority to SIP calls made to some specific numbers. The high priority is achieved by allocating bandwidth to such preferred SIP Calls even when there is no available voice bandwidth in the configured Voice Pool. This feature is supported only for those clients that use SIP based CAC for bandwidth allocation in WCS or WLC.
You can configure up to 6 numbers per controller.

To configure the preferred call support, follow these steps:

---

**Step 1** Choose *Configuration > Network > Network Devices*, then from the *Device Groups* menu on the left, select *Device Type > Wireless Controller*.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose 802.11 > **Preferred Call**. The following fields appear if there is an existing preferred call:
- Description—Description for the preferred call.
- Number Id—Indicates the unique identifier for the controller and denotes one of the six preferred call numbers assigned to the controller.
- Preferred Number—Indicates the preferred call number.

**Step 4** From the Select a command drop-down list, choose *Add Number*.

**Step 5** Select a template to apply to this controller.

You need to select a template to apply to the selected controller. To create a New Template for Preferred Call Numbers, see Configuring Preferred Call Templates in Related Topics.

**Step 6** Click *Apply*.

To delete a preferred call, select the check box for the applicable preferred call number and choose *Delete* from the Select a command drop-down list. Click *Go* and then click *OK* to confirm the deletion.

---

**Related Topics**
- Configuring General Parameters for 802.11 Controllers
- Configuring Aggressive Load Balancing
- Configuring Band Selection
- Configuring RF Profiles (802.11)

---

**Configuring 802.11 Media Parameters**

To configure media parameters for 802.11, follow these steps:

---

**Step 1** Choose *Configuration > Network > Network Devices*, then from the *Device Groups* menu on the left, select *Device Type > Wireless Controller*.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose 802.11 > **Media Stream**.

**Step 4** In the Media Stream Configuration section, configure the following parameters
- Media Stream Name
- Multicast Destination Start IP—Start IP address of the media stream to be multicast
- Multicast Destination End IP—End IP address of the media stream to be multicast
- Maximum Expected Bandwidth—Maximum bandwidth that a media stream can use

**Step 5** In the Resource Reservation Control (RRC) Parameters group box, configure the following parameters:
• Average Packet Size—Average packet size that a media stream can use.
• RRC Periodical Update—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
• RRC Priority—Priority of RRC with the highest at 1 and the lowest at 8.
• Traffic Profile Violation—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
• Policy—Appears if the media stream is admitted or denied.

Step 6 Click Save.

Configuring RF Profiles (802.11)

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups.

To configure a RF Profile for a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Click RF Profiles or choose either 802.11 > RF Profiles from the left sidebar menu. The RF Profiles page appears. This page lists the existing RF Profile templates.

Step 4 If you want to add a RF profile, choose Add RF Profile from the Select a command drop-down list.

Step 5 Click Go. The New Controller Template page appears.

Step 6 Configure the following information:

• General
  - Template Name—User-defined name for the template.
  - Profile Name—User-defined name for the current profile.
  - Description—Description of the template.
  - Radio Type—The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.

• TCP (Transmit Power Control)
  - Minimum Power Level Assignment (-10 to 30 dBm)—Indicates the minimum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Maximum Power Level Assignment (-10 to 30 dBm)—Indicates the maximum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Power Threshold v1(-80 to -50 dBm)—Indicates the transmitted power threshold.
  - Power Threshold v2(-80 to -50 dBm)—Indicates the transmitted power threshold.

• Data Rates—Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
  - 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
  - 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.

For each data rate, choose one of these options:
Configuring Controller Security Parameters

- Mandatory—Clients must support this data rate to associate to an access point on the controller.
- Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate.
- Disabled—The clients specify the data rates used for communication.

**Step 7** Click **Save**.

**Related Topics**
- Configuring General Parameters for 802.11 Controllers
- Configuring Aggressive Load Balancing
- Configuring Band Selection
- Configuring 802.11 Media Parameters

### Configuring SIP Snooping

Keep the following guidelines in mind when using SIP Snooping:

- SIPs are available only on the Cisco 5500 Series Controllers and on the 1240, 1130, and 11n access points.
- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

To configure SIP Snooping for a controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** Click the Device Name of the applicable controller.

**Step 4** From the left sidebar menu, choose **802.11 > SIP Snooping**.

**Step 5** Configure the following fields:
- Port Start
- Port End

If single port is to be used, configure both start and end port fields with same number.

**Step 6** Click **Save**.

**Related Topics**
- Configuring General Parameters for 802.11 Controllers
- Configuring Aggressive Load Balancing
- Configuring Band Selection
- Configuring 802.11 Media Parameters
Configuring 802.11a/n Parameters

- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
- Configuring 802.11a/n Roaming Parameters
- Configuring 802.11a/n 802.11h Parameters
- Configuring 802.11a/n High Throughput (802.11n) Parameters
- Configuring 802.11a/n CleanAir Parameters

**Configuring 802.11a/n General Parameters**

To view 802.11a/n parameters for a specific controller, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose 802.11a/n > Parameters to view the following parameters:

- **General**
  - 802.11a/n Network Status—Select the check box to enable.
  - Beacon Period—The amount of time between beacons. The valid range is from 100 to 600 milliseconds.
  - Fragmentation Threshold (in bytes)—The size at which packets are fragmented. Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
  - Template Applied

- **802.11a/n Band Status**
  - Low, Medium, and High Bands (read-only).

- **802.11a/n Power Status**
  - Dynamic Assessment—Automatic, On Demand, or Disabled.
  - Current Tx Level—Range includes: 1 (maximum power allowed per country code setting), 2 (50% power), 3 (25% power), 4 (6.25 to 12.5% power), and 5 (0.195 to 6.25% power). The power levels and available channels are defined by the country code setting and are regulated on a country by country basis.
  - Control Interval—in seconds (read-only).
  - Dynamic Treatment Power Control—Select the check box to enable.
• 802.11a/n Channel Status
  – Assignment Mode—Automatic, On Demand, or Disabled.
  – Update Interval—in seconds.
  – Avoid Foreign AP Interference—Enable to have RRM consider interference from foreign Cisco access points (those non-Cisco access points outside RF/mobility domain) when assigning channels.
  – Avoid Cisco AP load—Enable to have controllers consider the traffic bandwidth used by each access point when assigning channels to access points.
  – Avoid non 802.11 Noise—Enable to have access points avoid channels that have interference from non-access point sources, such as microwave ovens or Bluetooth devices. Disable this field to have RRM ignore this interference.
  – Signal Strength Contribution—Not configurable.
  – Avoid Persistent Non-WiFi interface

• Data Rates
  – Ranges between 6 Mbps and 54 Mbps—Supported, Mandatory, or Disabled.

• Noise/Interference/Rogue Monitoring Channels.
  – Channel List—All Channels, Country Channels, DCA Channels. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation from a set of managed devices connected to the controller.

• CCX Location Measurement—When enabled, it enhances the location accuracy of clients.
  – Mode—Select the check box to enable.
  – Interval—in seconds. The CCX Location Measurement Interval can be changed only when measurement mode is enabled.

**Step 4** Click **Save**.

**Related Topics**

- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
- Configuring 802.11a/n Roaming Parameters
- Configuring 802.11a/n 802.11h Parameters
- Configuring 802.11a/n High Throughput (802.11n) Parameters
- Configuring 802.11a/n CleanAir Parameters
Configuring 802.11a/n RRM Thresholds

To configure a 802.11a/n RRM threshold controller, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2  Click the device name of the applicable controller.

Step 3  From the left sidebar menu, choose 802.11a or n or ac > dot11a-RRM > RRM Thresholds.

Step 4  Coverage Hole Algorithm—Enter the values for the following parameters.

- In the Min Failed Clients field, enter the minimum number of failed clients currently associated with the controller.
- In the Coverage Level field, enter the target range of coverage threshold.
- In the Data RSSI field, enter the value in the specified range. This number indicated the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.
- In the Voice RSSI field, enter the value in the specified range. This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.

Step 5  Local Thresholds—Enter the values for the following parameters.

- In the Max Clients field, enter the maximum number of failed clients that are currently associated with the controller.
- In the RF Utilization field, enter the percentage of threshold for 802.11a/n.

Step 6  Threshold for Traps—Enter the values for the following parameters:

- In the Interference Threshold Percentage field, enter the percentage of interference threshold.
- In the Noise Threshold field, enter a noise threshold between -127 and 0dBm. When the controller is outside of this threshold, it sends an alarm to Prime Infrastructure.
- In the Coverage Exception Level per AP field, enter the percentage value of coverage exception level. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole generated.

Step 7  High Density Thresholds—Configure the following parameters.

- RX Sop Threshold—Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an AP radio demodulates and decodes a packet. If the RX Sop level is high, the radio becomes less sensitive and also the receiver cell size becomes small.
  From the RX Sop Threshold drop-down list, RX Sop Threshold, choose the threshold value. The possible values are Auto, Low, Medium, and High. Based on the RX Sop values, the radio dBM value changes.
- Optimized Roaming Mode—Enable or disable the Optimized Roaming Mode. You can configure Optimized Roaming Interval and Optimized Roaming Data Rate Threshold only if the Optimized Roaming Mode is enabled.
- Optimized Roaming Interval—Enter a value for optimized roaming interval. By default, the optimized roaming interval is 90 seconds. The range for optimized roaming interval is 5 to 90 seconds.
Chapter 27 Configuring Wireless Devices

Configuring Controller Security Parameters

- Optimized Roaming Data Rate Threshold—From the Optimized Roaming Data Rate Threshold drop-down list, choose the roaming data rate threshold value. The possible data rate threshold values are Disable, 6 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps. By default, the data rate is disabled.

**Step 8** Click **Save**.

**Related Topics**

- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
- Configuring 802.11a/n Roaming Parameters
- Configuring 802.11a/n 802.11h Parameters
- Configuring 802.11a/n High Throughput (802.11n) Parameters
- Configuring 802.11a/n CleanAir Parameters

### Configuring 802.11a/n RRM Intervals

To configure 802.11a/n or 802.11b/g/n RRM intervals for an individual controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **802.11a/n > RRM Intervals** or **802.11b/g/n > RRM Intervals**.

**Note** The default for the following four RRM interval parameters is 300 seconds.

**Step 4** Enter at which interval you want strength measurements taken for each access point.

**Step 5** Enter at which interval you want noise and interference measurements taken for each access point.

**Step 6** Enter at which interval you want load measurements taken for each access point.

**Step 7** Enter at which interval you want coverage measurements taken for each access point.

**Step 8** Click **Save**.

**Related Topics**

- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Thresholds
The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of the access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

Transmit Power Control version 2 (TPCv2) attempts to reduce the co-channel interference from Cisco AP networks. The former version of TPC is designed to provide strong signal coverage with a tendency to use larger Tx Power, and as a result customers were suffering from overheating in densely deployed networks.

To configure 802.11a/n or 802.11b/g/n RRM TPC, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **802.11a/n-RRM > TPC**.

**Step 4** Configure the following TPC parameters:

- **Template Applied**—The name of the template applied to this controller.
- **Template Version**—Indicates the TPC version.
  
  The TPCv2 option is applicable only for those controllers running 7.2.x release or later.
- **Dynamic Assignment**—At the Dynamic Assignment drop-down list, choose one of three modes:
  
  - **Automatic** - The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand** - Transmit power is updated when the Assign Now button is selected.
  - **Disabled** - No dynamic transmit power assignments occur, and values are set to their global default.
Configuring Controller Security Parameters

- Maximum Power Assignment—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Minimum Power Assignment—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- Dynamic Tx Power Control—Determine if you want to enable Dynamic Tx Power Control.
- Transmitted Power Threshold—Enter a transmitted power threshold between -50 and -80.
- Control Interval—in seconds (read-only).

Step 5 Click Save.

Related Topics
- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Thresholds
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
- Configuring 802.11a/n Roaming Parameters
- Configuring 802.11a/n 802.11h Parameters
- Configuring 802.11a/n High Throughput (802.11n) Parameters
- Configuring 802.11a/n CleanAir Parameters

Configuring 802.11a/n/ac RRM Dynamic Channel Allocation

The Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) page allows you to choose the DCA channels as well as the channel width for this controller.

RRM DCA supports 802.11n 40-MHz channel width in the 5-GHz band. The higher bandwidth allows radios to achieve higher instantaneous data rates. Choosing a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments. To view the channel width for the radio of an access point, go to Monitor > Network Devices > Access Points > name > Interfaces tab. You can also view the channel width and antenna selections by choosing Configuration > Network > Network Devices > Access Points and clicking the desired radio in the Radio column.

To configure 802.11 a/n RRM DCA channels for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.
Chapter 27  Configuring Wireless Devices

Configuring Controller Security Parameters

Step 3  From the left sidebar menu, choose 802.11a or n or ac >dot11a-RRM > DCA. The 802.11a/n RRM DCA page appears.

You can also configure the channel width on the access point page by choosing Configure > Access Points, and clicking the 802.11a/n/ac link in the Radio column. The Current RF Channel Assignment is provided, and you can choose a Global assignment method or choose Custom to specify a channel.

Step 4  From the Channel Width drop-down list, choose 20 MHz or 40 MHz. Prior to software release 5.1, 40-MHz channels were only statically configurable. Only radios with 20-MHz channels were supported by DCA. With 40 MHz, radios can achieve higher instantaneous data rates; however, larger bandwidths reduce the number of non-overlapping channels so certain deployments could have reduced overall network throughput.

Note  Be cautious about deploying a mix of 20-MHz and 40-MHz devices. The 40-MHz devices have slightly different channel access rules which might negatively impact the 20-MHz devices.

Step 5  Select the check boxes for the appropriate DCA channels. The selected channels are listed in the Selected DCA channels list.

Step 6  Enable or disable event-driven Radio Resource Management (RRM) using the following parameters. Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference.

- Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
- Sensitivity Threshold—If Event Driven RRM is enabled, this field displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.
- Rogue Contribution—Rogue Contribution can be enabled only if the Event Driven RRM configuration is enabled. Select the Rogue Contribution check box to enable contribution from the rogue access points.
- Rogue Duty-Cycle—If the Rogue Contribution is enabled, Rogue Duty-Cycle field displays the interval at which the rogue access points are interfered. Select how much duty cycle you should consider for event driven RRM to trigger. Once it crosses the specified the duty-cycle percentage, it triggers the event driven RRM. The range is 1 to 99 percentage.

Step 7  Click Save.

Related Topics
- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Thresholds
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
Configuring 802.11a/n RRM Radio Grouping

To configure 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2  Click the device name of the applicable controller.

Step 3  From the left sidebar menu, choose 802.11a/n > RRM > RF Grouping.

Step 4  Choose a grouping mode from the drop-down list. The following parameters appear:
- Automatic—Allows you to activate the automatic RRM Grouping Algorithm. This is the default mode.
- Off—Allows you to deactivate the automatic grouping.
- Leader—Allows you to assign members to the group.

Step 5  Choose a group update interval (secs) from the drop-down list. When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. The grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. Default value is 600 seconds.

Step 6  In the Group Members group box, click Add >. The selected controller moves from the Available Controllers to the RF Group Members list.

The RF Group Members group box appears only when the grouping mode is set to Leader. The maximum number of controllers that can be added to a RF Group is 20.

Step 7  Click Save.

Related Topics
- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Thresholds
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
- Configuring 802.11a/n Roaming Parameters
- Configuring 802.11a/n High Throughput (802.11n) Parameters
- Configuring 802.11a/n CleanAir Parameters
To configure the media parameters for 802.11a/n, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose 802.11a/n > Media Parameters.

**Step 4** On the Voice tab, configure the following parameters:

- **Admission Control (ACM)**—Select the check box to enable admission control.
  
  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- **CAC Method**—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.
  
  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.
  
  In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

- **Maximum Bandwidth Allowed**—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. The valid range is 5 to 85.

- **Reserved Roaming Bandwidth**—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25.

- **Expedited Bandwidth**—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.
  
  You must have an expedited bandwidth that is CCXv5 compliant so that a TSPEC request is given higher priority.

- **SIP CAC**—Select the check box to enable SIP CAC.
  
  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- **SIP Codec**—Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.

- **SIP Call Bandwidth**—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.
• SIP Sample Interval—Specify the sample interval in milliseconds that the codec must operate in.
• Max Voice Calls per Radio—Specify the maximum number of voice calls that can be made per Radio.
• Max Roaming Reserved Calls per Radio—Specify the maximum number of roaming calls that can be reserved per Radio. The Max Voice Calls per Radio and Max Roaming Reserved Calls per Radio options are available only if the CAC Method is specified as Static and SIP CAC is enabled.
• Metric Collection—Select the check box to enable metric collection.

Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

Step 5 On the Video tab, configure the following parameters:
• Admission Control (ACM)—Select the check box to enable admission control.
• Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. For controller versions 6.0.188.0 and earlier, the valid range is 0 to 100. For controller versions 6.0.188.1 and later, the valid range is 5 to 85.
• Reserved Roaming Bandwidth—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25, and the default is 0.
• Static CAC method—From the SIP Codec drop-down list, choose one of the following options to set the CAC method. The default value is G.711. The options are as follows:
  – Load-Based
  – Static

Static CAC method is radio based and load-based CAC method is channel based
• SIP CAC—Select the SIP CAC check box to enable Static CAC support. By default, this check box is disabled. SIP CAC will be supported only if SIP snooping is enabled. SIPs are available only on the following controllers: 4400, 5500. Also, SIPs are available only for the following access points: 1240, 1130, and 11n.
• Unicast Video Redirect—Select the Unicast Video Redirect check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.
• Client Minimum Phy Rate—Choose the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.
• Multicast Direct Enable—Select the Multicast Direct Enable check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.
• Maximum Number of Streams per Radio—Specify the maximum number of streams per Radio to be allowed.
• Maximum Number of Streams per Client—Specify the maximum number of streams per Client to be allowed.
• Best Effort QOS Admission—Select the Best Effort QOS Admission check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used. If disabled and maximum video bandwidth has been used, then any new client request is rejected.

Step 6 On the General tab, configure the following field:
• Maximum Media Bandwidth (0 to 85%)—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

Step 7 Click Save.

Related Topics
• Configuring 802.11a/n General Parameters
• Configuring 802.11a/n RRM Thresholds
• Configuring 802.11a/n RRM Intervals
• Configuring 802.11a/n RRM Transmit Power Control
• Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
• Configuring 802.11a/n RRM Radio Grouping
• Configuring 802.11a/n EDCA Parameters
• Configuring 802.11a/n Roaming Parameters
• Configuring 802.11a/n 802.11h Parameters
• Configuring 802.11a/n High Throughput (802.11n) Parameters
• Configuring 802.11a/n CleanAir Parameters

Configuring 802.11a/n EDCA Parameters

The EDCA parameters (EDCA profile and Streaming MAC Enable settings) for 802.11a/n and 802.11b/g/n can be configured either by individual controller or through a controller template to improve voice QoS support.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11a/n > EDCA Parameters or 802.11b/g/n > EDCA Parameters.

Step 4 Choose the EDCA Profile from the drop-down list.

Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile. You must shut down radio interface before configuring EDCA Parameters.

Step 5 Select the Enable Streaming MAC check box to enable this feature.

Only enable Streaming MAC if all clients on the network are WMM compliant.

Related Topics
• Configuring 802.11a/n General Parameters
• Configuring 802.11a/n RRM Thresholds
• Configuring 802.11a/n RRM Intervals
Chapter 27      Configuring Wireless Devices

Configuring Controller Security Parameters

- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n Roaming Parameters
- Configuring 802.11a/n 802.11h Parameters
- Configuring 802.11a/n CleanAir Parameters

Configuring 802.11a/n Roaming Parameters

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11a/n > Roaming Parameters.

Step 4 From the Mode drop-down list, choose Default values or Custom values.
- Default values—The default values (read-only) are automatically displayed in the text boxes.
- Custom values—Activates the text boxes to enable editing of the roaming parameters.

Step 5 In the Minimum RSSI text box, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.
- Range: -80 to -90 dBm
- Default: -85 dBm

If the client average received signal power dips below this threshold, reliable communication is typically impossible; clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Step 6 In the Hysteresis text box, enter a value to indicate how strong the signal strength of a neighboring access point must for the client to roam to it.

This field is intended to reduce the amount of “ping ponging” between access points if the client is physically located on or near the border between two access points.
- Range: 2 to 4 dB
- Default: 3 dB

Step 7 In the Adaptive Scan Threshold text box, enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.

This field provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.
- Range: -70 to -77 dB
- Default: -72 dB
Step 8 In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

- Range: 1 to 10 seconds
- Default: 5 seconds

Step 9 Click Save.

Related Topics
- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Thresholds
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
- Configuring 802.11a/n 802.11h Parameters
- Configuring 802.11a/n High Throughput (802.11n) Parameters
- Configuring 802.11a/n CleanAir Parameters

Configuring 802.11a/n 802.11h Parameters

To configure 802.11h parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11a/n > 802.11h or 802.11b/g/n > 802.11h.

Step 4 Select the power constraint check box to enable TPC.

Step 5 Select the channel announcement check box to enable channel announcement. Channel announcement is a method in which the access point announces when it is switching to a new channel and the new channel number.

Step 6 Click Save.

Related Topics
- Configuring 802.11a/n General Parameters
To configure 802.11a/n or 802.11b/g/n high throughput parameters, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose 802.11a/n > High Throughput or 802.11b/g/n > High Throughput.

**Step 4** Select the 802.11n Network Status Enabled check box to enable high throughput.

**Step 5** In the MCS (Data Rate) Settings, choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used. When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

**Step 6** Click Save.

**Related Topics**
- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Thresholds
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
- Configuring 802.11a/n Roaming Parameters
- Configuring 802.11a/n High Throughput (802.11n) Parameters
- Configuring 802.11a/n CleanAir Parameters
Configuring 802.11a/n CleanAir Parameters

To configure 802.11a/n CleanAir parameters, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose 802.11a/n > CleanAir to view the following information.

- **CleanAir**—Select the check box to enable CleanAir functionality on the 802.11 a/n network, or unselect to disable CleanAir functionality. The default value is selected.

- **Reporting Configuration**—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  
  - Report—Select the report interferers check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect text box and any that do not need to be detected appear in the Interferers to Ignore text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources are detected.
  
  - Select the Persistent Device Propagation check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points. Persistent interferers are present at the a location and interfere with the WLAN operations even if they are not detectable at all times.

- **Alarm Configuration**—This section enables you to configure triggering of air quality alarms.
  
  - Air Quality Alarm—Select the Air Quality Alarm check box to enable the triggering of air quality alarms, or unselect the box to disable this feature. The default value is selected.
  
  - Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default is 35.
  
  - Air Quality Unclassified category Alarm—Select the Air Quality Unclassified category Alarm check box to enable the alarms to be generated for unclassified interference category. CleanAir can detect and monitor unclassified interferences. Unclassified interference are interference that are detected but do not correspond to any of the known interference types. The Unclassified category alarm is generated when the unclassified severity goes above the configured threshold value for unclassified severity or when the air quality index goes below the configured threshold value for Air Quality Index.

  - Air Quality Unclassified Category Severity Threshold—If you selected the Air Quality Unclassified category Alarm check box, enter a value between 1 and 99 (inclusive) in the Air Quality Unclassified Severity Threshold text box to specify the threshold at which you want the unclassified category alarm to be triggered. The default is 20.

  - Interferers For Security Alarm—Select the Interferers For Security Alarm check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.
- Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms text box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms text box. Use the > and < buttons to move interference sources between these two boxes. By default, all interference sources trigger interferer alarms.

- Event Driven RRM—To trigger spectrum event-driven Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, follow these steps:
  - Event Driven RRM—Displays the current status of spectrum event-driven RRM.
  - Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

---

**Related Topics**

- Configuring 802.11a/n General Parameters
- Configuring 802.11a/n RRM Thresholds
- Configuring 802.11a/n RRM Intervals
- Configuring 802.11a/n RRM Transmit Power Control
- Configuring 802.11a/n/ac RRM Dynamic Channel Allocation
- Configuring 802.11a/n RRM Radio Grouping
- Configuring 802.11a/n Media Parameters
- Configuring 802.11a/n EDCA Parameters
- Configuring 802.11a/n Roaming Parameters
- Configuring 802.11a/n 802.11h Parameters
- Configuring 802.11a/n High Throughput (802.11n) Parameters
- Configuring 802.11b/g/n CleanAir Parameters

---

**Configuring 802.11b/g/n General Parameters**

To view 802.11b/g/n parameters for a specific controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **802.11b/g/n Parameters** to view the following parameters:

- **General**
  - 802.11b/g Network Status—Select the check box to enable.
  - 802.11g Support—Select the check box to enable.
  - Beacon Period—In milliseconds.
DTIM Period—The number of beacon intervals that might elapse between transmission of beacon frames containing a traffic indicator message (TIM) element whose delivery count field is 0.

Fragmentation Threshold—In bytes.

Short Preamble—Select the check box to enable.

Template Applied.

- **802.11a/n Power Status**
  - Dynamic Assessment—Automatic, On Demand, or Disabled.
  - Current Tx Level.
  - Control Interval—In seconds (Read-only).
  - Dynamic Treatment Power Control—Select the check box to enable.

- **802.11a/n Channel Status**
  - Assignment Mode—Automatic, On Demand, or Disabled.
  - Update Interval—In seconds.
  - Avoid Foreign AP Interference—Select the check box to enable.
  - Avoid Cisco AP load—Select the check box to enable.
  - Avoid non 802.11 Noise—Select the check box to enable.
  - Signal Strength Contribution—Select the check box to enable.

- **Data Rates**
  - Ranges between 1 Mbps and 54 Mbps—Supported, Mandatory, or Disabled.

- **Noise/Interference/Rogue Monitoring Channels**
  - Channel List—All Channels, Country Channels, DCA Channels.

- **CCX Location Measurement**
  - Mode—Select the check box to enable.
  - Interval—In seconds.
  
  The CCX Location Measurement Interval can be changed only when measurement mode is enabled.

**Step 4**

Click **Save**.

---

**Related Topics**

- Configuring 802.11b/g/n RRM Thresholds
- Configuring 802.11b/g/n RRM Intervals
- Configuring 802.11b/g/n RRM Transmit Power Control
- Configuring 802.11b/g/n RRM DCA
- Configuring 802.11b/g/n RRM Radio Grouping
- Configuring 802.11b/g/n Media Parameters
- Configuring 802.11b/g/n EDCA Parameters
- Configuring 802.11b/g/n Roaming Parameters
- Configuring 802.11b/g/n High Throughput (802.11n) Parameters
• Configuring 802.11b/g/n CleanAir Parameters

Configuring 802.11b/g/n RRM Thresholds

To configure a 802.11b/g/n RRM threshold controller, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2  Click the device name of the applicable controller.

Step 3  From the left sidebar menu, choose 802.11b or g or n > dot11b-RRM > Thresholds.

Step 4  Coverage Hole Algorithm—Enter the values for the following parameters.

• In the Min Failed Clients field, enter the minimum number of failed clients currently associated with the controller.

• In the Coverage Level field, enter the target range of coverage threshold.

• In the Data RSSI field, enter the value in the specified range. This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) for data required for the client to associate to an access point.

• In the Voice RSSI field, enter the value in the specified range. This number indicates the value for the minimum Received Signal Strength Indicator (RSSI) required for voice for the client to associate to an access point.

Step 5  Local Thresholds—Enter the values for the following parameters.

• In the Max Clients field, enter the maximum number of failed clients that are currently associated with the controller.

• In the RF Utilization field, enter the percentage of threshold for 802.11a/n.

Step 6  Threshold for Traps—Enter the values for the following parameters.

• In the Interference Threshold Percentage field, enter the percentage of interference threshold.

• In the Noise Threshold field, enter a noise threshold between -127 and 0 dBm. When the controller is outside of this threshold, it sends an alarm to Prime Infrastructure.

• In the Coverage Exception Level per AP field, enter the percentage value of coverage exception level. When the coverage drops by this percentage from the configured coverage for the minimum number of clients, a coverage hole is generated.

Step 7  High Density Thresholds—Configure the following parameters.

• RX Sop Threshold—Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an AP radio demodulates and decodes a packet. If the RX Sop level is high, the radio becomes less sensitive and also the receiver cell size becomes small.

  From the RX Sop Threshold drop-down list, RX Sop Threshold, choose the threshold value. The possible values are Auto, Low, Medium, and High. Based on the RX Sop values, the radio dBM value changes.

• Optimized Roaming Mode—Enable or disable the Optimized Roaming Mode. You can configure Optimized Roaming Interval and Optimized Roaming Data Rate Threshold only if the Optimized Roaming Mode is enabled.
• Optimized Roaming Interval—Enter a value for optimized roaming interval. By default, the optimized roaming interval is 90 seconds. The range for optimized roaming interval is 5 to 90 seconds.

• Optimized Roaming Data Rate Threshold—From the Optimized Roaming Data Rate Threshold drop-down list, choose the roaming data rate threshold value. The possible data rate threshold values are Disable, 6 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps. By default, the data rate is disabled.

Step 8  Click Save.

Related Topics
• Configuring 802.11b/g/n General Parameters
• Configuring 802.11b/g/n RRM Intervals
• Configuring 802.11b/g/n RRM Transmit Power Control
• Configuring 802.11b/g/n RRM DCA
• Configuring 802.11b/g/n RRM Radio Grouping
• Configuring 802.11b/g/n Media Parameters
• Configuring 802.11b/g/n EDCA Parameters
• Configuring 802.11b/g/n Roaming Parameters
• Configuring 802.11b/g/n High Throughput (802.11n) Parameters
• Configuring 802.11b/g/n CleanAir Parameters

Configuring 802.11b/g/n RRM Intervals

To configure 802.11a/n or 802.11b/g/n RRM intervals for an individual controller, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2  Click the device name of the applicable controller.

Step 3  From the left sidebar menu, choose 802.11a/n > RRM Intervals or 802.11b/g/n > RRM Intervals.

Note  The default for the following four RRM interval parameters is 300 seconds.

Step 4  Enter at which interval you want strength measurements taken for each access point.

Step 5  Enter at which interval you want noise and interference measurements taken for each access point.

Step 6  Enter at which interval you want load measurements taken for each access point.

Step 7  Enter at which interval you want coverage measurements taken for each access point.

Step 8  Click Save.

Related Topics
• Configuring 802.11b/g/n General Parameters
Configuring 802.11b/g/n RRM Transmit Power Control

The controller dynamically controls access point transmit power based on real-time wireless LAN conditions. Normally, power can be kept low to gain extra capacity and reduce interference. The controller attempts to balance the transmit power of an access point according to how the access points are seen by their third strongest neighbor.

The transmit power control (TPC) algorithm both increases and decreases the power of an access point in response to changes in the RF environment. In most instances, TPC seeks to lower the power of an access point to reduce interference, but in the case of a sudden change in the RF coverage—for example, if an access point fails or becomes disabled—TPC can also increase power on surrounding access points. This feature is different from Coverage Hole Detection. Coverage hole detection is primarily concerned with clients, while TPC is tasked with providing enough RF power to achieve desired coverage levels while avoiding channel interference between access points.

To configure 802.11b/g/n RRM TPC, follow these steps:

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose 802.11b/g/n-RRM > TPC.

**Step 4** Configure the following TPC parameters:

- **Template Applied**—The name of the template applied to this controller.
- **Dynamic Assignment**—At the Dynamic Assignment drop-down list, choose one of three modes:
  - **Automatic**—The transmit power is periodically updated for all access points that permit this operation.
  - **On Demand**—Transmit power is updated when the Assign Now button is selected.
  - **Disabled**—No dynamic transmit power assignments occur, and values are set to their global default.
- **Maximum Power Assignment**—Indicates the maximum power assigned.
  - Range: -10 to 30 dB
  - Default: 30 dB
- **Minimum Power Assignment**—Indicates the minimum power assigned.
  - Range: -10 to 30 dB
Step 5 Click Save.

Related Topics
- Configuring 802.11b/g/n General Parameters
- Configuring 802.11b/g/n RRM Thresholds
- Configuring 802.11b/g/n RRM Intervals
- Configuring 802.11b/g/n RRM DCA
- Configuring 802.11b/g/n RRM Radio Grouping
- Configuring 802.11b/g/n Media Parameters
- Configuring 802.11b/g/n EDCA Parameters
- Configuring 802.11b/g/n Roaming Parameters
- Configuring 802.11b/g/n High Throughput (802.11n) Parameters
- Configuring 802.11b/g/n CleanAir Parameters

Configuring 802.11b/g/n RRM DCA

To configure 802.11a/n or 802.11b/g/n RRM DCA channels for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11b or g or n > dot11b-RRM > DCA

Step 4 Select the check box(es) for the applicable DCA channel(s). The selected channels are listed in the Selected DCA channels text box.

Step 5 Enable or disable event-driven Radio Resource Management (RRM). Event Driven RRM is used when a CleanAir-enabled access point detects a significant level of interference, follow these steps:
- Event Driven RRM—Enable or Disable spectrum event-driven RRM. By default, Event Driven RRM is enabled.
- Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Assignment (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.
- Rogue Contribution—Rogue Contribution can be enabled only if the Event Driven RRM configuration is enabled. Select the Rogue Contribution check box to enable contribution from rogue access points.
Configuring Wireless Devices

Chapter 27

Configuring Controller Security Parameters

- Rogue Duty-Cycle—If the Rogue Contribution is enabled, **Rogue Duty-Cycle** field displays the interval at which the rogue access points are interfered. Select how much duty cycle you should consider for event driven RRM to trigger. Once it crosses the specified the duty-cycle percentage, it triggers the event driven RRM. The range is 1 to 99 percentage.

**Step 6** Click *Save*.

---

**Related Topics**

- Configuring 802.11b/g/n General Parameters
- Configuring 802.11b/g/n RRM Thresholds
- Configuring 802.11b/g/n RRM Intervals
- Configuring 802.11b/g/n RRM Transmit Power Control
- Configuring 802.11b/g/n RRM Radio Grouping
- Configuring 802.11b/g/n Media Parameters
- Configuring 802.11b/g/n EDCA Parameters
- Configuring 802.11b/g/n Roaming Parameters
- Configuring 802.11b/g/n High Throughput (802.11n) Parameters
- Configuring 802.11b/g/n CleanAir Parameters

---

### Configuring 802.11b/g/n RRM Radio Grouping

To configure 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller, follow these steps:

**Step 1** Choose *Configuration > Network > Network Devices*, then from the *Device Groups* menu on the left, select *Device Type > Wireless Controller*.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **802.11b/g/n > RRM > RF Grouping**.

**Step 4** Choose a grouping mode from the drop-down list. The following parameters appear:

- **Automatic**—Allows you to activate the automatic RRM Grouping Algorithm. This is the default mode.
- **Off**—Allows you to deactivate the automatic grouping.
- **Leader**—Allows you to assign members to the group.

**Step 5** Choose a group update interval (secs) from the drop-down list. When grouping is on, this interval (in seconds) represents the period with which the grouping algorithm is run by the Group Leader. Grouping algorithm also runs when the group contents changes and the automatic grouping is enabled. A dynamic grouping can be started upon request from the system administrator. The default value is 600 seconds.

**Step 6** In the Group Members group box, click *Add >*. The selected controller moves from the Available Controllers to the RF Group Members list.

The RF Group Members group box appears only when the grouping mode is set to Leader. The maximum number of controllers that can be added to a RF Group is 20.
Step 7 Click Save.

Related Topics
- Configuring 802.11b/g/n General Parameters
- Configuring 802.11b/g/n RRM Thresholds
- Configuring 802.11b/g/n RRM Intervals
- Configuring 802.11b/g/n RRM Transmit Power Control
- Configuring 802.11b/g/n RRM DCA
- Configuring 802.11b/g/n Media Parameters
- Configuring 802.11b/g/n EDCA Parameters
- Configuring 802.11b/g/n Roaming Parameters
- Configuring 802.11b/g/n High Throughput (802.11n) Parameters
- Configuring 802.11b/g/n CleanAir Parameters

Configuring 802.11b/g/n Media Parameters

To configure the media parameters for 802.11b/g/n, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11b/g/n > Media Parameters.

Step 4 In the Voice tab, configure the following parameters:

- Admission Control (ACM)—Select the check box to enable admission control.
  
  For end users to experience acceptable audio quality during a VoIP phone call, packets must be delivered from one endpoint to another with low latency and low packet loss. To maintain QoS under differing network loads, Call Admission Control (CAC) is required. CAC on an access point allows it to maintain controlled QoS when the network is experiencing congestion and keep the maximum allowed number of calls to an acceptable quantity.

- CAC Method—If Admission Control (ACM) is enabled, specify the CAC method as either load-based or static.
  
  Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by co-located channel interference. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

  In load-based CAC, the access point periodically measures and updates the utilization of the RF channel, channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents over-subscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

- Maximum Bandwidth Allowed—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. The valid range is 5 to 85.
Configuring Controller Security Parameters

- **Reserved Roaming Bandwidth**—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25.

- **Expedited Bandwidth**—Select the check box to enable expedited bandwidth as an extension of CAC for emergency calls.

  You must have an expedited bandwidth that is CCXv5 compliant so that a TSPEC request is given higher priority.

- **SIP CAC**—Select the check box to enable SIP CAC.

  SIP CAC should be used only for phones that support status code 17 and do not support TSPEC-based admission control.

- **SIP Codec**—Specify the codec name you want to use on this radio. The available options are G.711, G.729, and User Defined.

- **SIP Call Bandwidth**—Specify the bandwidth in kilobits per second that you want to assign per SIP call on the network. This field can be configured only when the SIP Codec selected is User Defined.

- **SIP Sample Interval**—Specify the sample interval in milliseconds that the codec must operate in.

- **Max Voice Calls per Radio**—Indicates the maximum number of voice calls that can be made per Radio. You cannot set the value of Max Voice Calls per Radio. This is automatically calculated based on the selected CAC method, Max BW allowed, and Roaming Bandwidth.

- **Max Roaming Reserved Calls per Radio**—Indicates the maximum number roaming calls that can be reserved per Radio. The Max Voice Calls per Radio and Max Roaming Reserved Calls per Radio options are available only if the CAC Method is specified as Static and SIP CAC is enabled.

- **Metric Collection**—Select the check box to enable metric collection.

  Traffic stream metrics are a series of statistics about VoIP over your wireless LAN which inform you of the QoS of the wireless LAN. For the access point to collect measurement values, traffic stream metrics must be enabled. When this is enabled, the controller begins collecting statistical data every 90 seconds for the 802.11b/g interfaces from all associated access points. If you are using VoIP or video, this feature should be enabled.

**Step 5**

In the **Video** tab, configure the following parameters:

- **Admission Control (ACM)**—Select the check box to enable admission control.

- **Maximum Bandwidth**—Specify the percentage of maximum bandwidth allowed. This option is only available when CAC is enabled. For controller versions 6.0.188.0 and earlier, the valid range is 0 to 100. For controller versions 6.0.188.1 and later, the valid range is 5 to 85.

- **Reserved Roaming Bandwidth**—Specify the percentage of reserved roaming bandwidth. This option is only available when CAC is enabled. The valid range is 0 to 25.

- **Unicast Video Redirect**—Select the **Unicast Video Redirect** check box to enable all non-media stream packets in video queue are redirected to the best effort queue. If disabled, all packets with video marking are kept in video queue.

- **Client Minimum Phy Rate**—Specify the physical data rate required for the client to join a media stream from the Client Minimum Phy Rate drop-down list.

- **Multicast Direct Enable**—Select the **Multicast Direct Enable** check box to set the Media Direct for any WLAN with Media Direct enabled on a WLAN on this radio.

- **Maximum Number of Streams per Radio**—Specify the maximum number of streams per Radio to be allowed.

- **Maximum Number of Streams per Client**—Specify the maximum number of streams per Client to be allowed.
- Best Effort QOS Admission—Select the **Best Effort QOS Admission** check box to redirect new client requests to the best effort queue. This happens only if all the video bandwidth has been used. If disabled and maximum video bandwidth has been used, then any new client request is rejected.

**Step 6** On the **General** tab, configure the following field:
- **Maximum Media Bandwidth (0 to 85%)**—Specify the percentage of maximum of bandwidth allowed. This option is only available when CAC is enabled.

**Step 7** Click **Save**.

---

**Related Topics**
- Configuring 802.11b/g/n General Parameters
- Configuring 802.11b/g/n RRM Thresholds
- Configuring 802.11b/g/n RRM Intervals
- Configuring 802.11b/g/n RRM Transmit Power Control
- Configuring 802.11b/g/n RRM DCA
- Configuring 802.11b/g/n RRM Radio Grouping
- Configuring 802.11b/g/n EDCA Parameters
- Configuring 802.11b/g/n Roaming Parameters
- Configuring 802.11b/g/n High Throughput (802.11n) Parameters
- Configuring 802.11b/g/n CleanAir Parameters

---

**Configuring 802.11b/g/n EDCA Parameters**

The EDCA parameters (EDCA profile and Streaming MAC Enable settings) for 802.11a/n and 802.11b/g/n can be configured either by individual controller or through a controller template to improve voice QoS support.

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **802.11a/n > EDCA Parameters** or **802.11b/g/n > EDCA Parameters**.

**Step 4** Choose the EDCA Profile from the drop-down list.
Profiles include Wi-Fi Multimedia (WMM), Spectralink Voice Priority (SVP), Voice Optimized, and Voice & Video Optimized. WMM is the default EDCA profile. You must shut down radio interface before configuring EDCA Parameters.

**Step 5** Select the **Enable Streaming MAC** check box to enable this feature.

Only enable Streaming MAC if all clients on the network are WMM compliant.
Chapter 27 Configuring Wireless Devices

Configuring Controller Security Parameters

Related Topics
- Configuring 802.11b/g/n General Parameters
- Configuring 802.11b/g/n RRM Thresholds
- Configuring 802.11b/g/n RRM Intervals
- Configuring 802.11b/g/n RRM Transmit Power Control
- Configuring 802.11b/g/n RRM DCA
- Configuring 802.11b/g/n RRM Radio Grouping
- Configuring 802.11b/g/n Media Parameters
- Configuring 802.11b/g/n Roaming Parameters
- Configuring 802.11b/g/n High Throughput (802.11n) Parameters
- Configuring 802.11b/g/n CleanAir Parameters

Configuring 802.11b/g/n Roaming Parameters

To configure 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller, follow these steps:

---

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11a/n > Roaming Parameters or 802.11b/g/n > Roaming Parameters.

Step 4 From the Mode drop-down list, choose Default values or Custom values.
- Default values—The default values (read-only) are automatically displayed in the text boxes.
- Custom values—Activates the text boxes to enable editing of the roaming parameters.

Step 5 In the Minimum RSSI text box, enter a value for the minimum Received Signal Strength Indicator (RSSI) required for the client to associate to an access point.
- Range: -80 to -90 dBm
- Default: -85 dBm

Note: If the client average received signal power dips below this threshold, reliable communication is typically impossible; clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

Step 6 In the Hysteresis text box, enter a value to indicate how strong the signal strength of a neighboring access point must be in order for the client to roam to it.

This field is intended to reduce the amount of “ping ponging” between access points if the client is physically located on or near the border between two access points.
- Range: 2 to 4 dB
- Default: 3 dB

Step 7 In the Adaptive Scan Threshold text box, enter the RSSI value, from a client associated access point, below which the client must be able to roam to a neighboring access point within the specified transition time.
This field provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when below the threshold.

- Range: -70 to -77 dB
- Default: -72 dB

**Step 8**

In the Transition Time text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

- Range: 1 to 10 seconds
- Default: 5 seconds

**Step 9**

Click **Save**.

**Related Topics**

- Configuring 802.11b/g/n General Parameters
- Configuring 802.11b/g/n RRM Thresholds
- Configuring 802.11b/g/n RRM Intervals
- Configuring 802.11b/g/n RRM Transmit Power Control
- Configuring 802.11b/g/n RRM DCA
- Configuring 802.11b/g/n RRM Radio Grouping
- Configuring 802.11b/g/n Media Parameters
- Configuring 802.11b/g/n EDCA Parameters
- Configuring 802.11b/g/n High Throughput (802.11n) Parameters
- Configuring 802.11b/g/n CleanAir Parameters

**Configuring 802.11b/g/n High Throughput (802.11n) Parameters**

To configure 802.11a/n or 802.11b/g/n high throughput parameters, follow these steps:

**Step 1**

Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2**

Click the device name of the applicable controller.

**Step 3**

From the left sidebar menu, choose **802.11a/n > High Throughput** or **802.11b/g/n > High Throughput**.

**Step 4**

Select the **802.11n Network Status Enabled** check box to enable high throughput.

**Step 5**

In the MCS (Data Rate) Settings, choose which level of data rate you want supported. MCS is modulation coding schemes which are similar to 802.11a data rate. As a default, 20 MHz and short guarded interval is used.
When you select the Supported check box, the chosen numbers appear in the Selected MCS Indexes page.

Step 6 Click **Save**.

---

**Related Topics**

- Configuring 802.11b/g/n General Parameters
- Configuring 802.11b/g/n RRM Thresholds
- Configuring 802.11b/g/n RRM Intervals
- Configuring 802.11b/g/n RRM Transmit Power Control
- Configuring 802.11b/g/n RRM DCA
- Configuring 802.11b/g/n RRM Radio Grouping
- Configuring 802.11b/g/n Media Parameters
- Configuring 802.11b/g/n EDCA Parameters
- Configuring 802.11b/g/n Roaming Parameters
- Configuring 802.11b/g/n CleanAir Parameters

---

**Configuring 802.11b/g/n CleanAir Parameters**

To configure 802.11b/g/n CleanAir parameters, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **802.11b/g/n > CleanAir** to view the following information.

- **CleanAir**—Select the check box to enable CleanAir functionality on the 802.11b/g/n network, or unselect to prevent the controller from detecting spectrum interference. The default value is selected.

- **Reporting Configuration**—Use the parameters in this section to configure the interferer devices you want to include for your reports.
  
  - **Report**—Select the **report interferers** check box to enable CleanAir system to report and detect sources of interference, or unselect it to prevent the controller from reporting interferers. The default value is selected.
  
  - Make sure that any sources of interference that need to be detected and reported by the CleanAir system appear in the Interferences to Detect text box and any that do not need to be detected appear in the Interferers to Ignore text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources are detected.

  - Select the **Persistent Device Propagation** check box to enable propagation of information about persistent devices that can be detected by CleanAir. Persistent device propagation enables designating information about interference types and propagating this information to the neighboring access points. Persistent interferers are present at a location and interfere with the WLAN operations even if they are not detectable at all times.

  - **Alarm Configuration**—This group box enables you to configure triggering of air quality alarms.
– Air Quality Alarm—Select the **Air Quality Alarm** check box to enable the triggering of air quality alarms, or unselect the text box to disable this feature. The default value is selected.

– Air Quality Alarm Threshold—If you selected the Air Quality Alarm check box, enter a value between 1 and 100 (inclusive) in the Air Quality Alarm Threshold text box to specify the threshold at which you want the air quality alarm to be triggered. When the air quality falls below the threshold level, the alarm is triggered. A value of 1 represents the worst air quality, and 100 represents the best. The default value is 35.

– Air Quality Unclassified category Alarm—Select the **Air Quality Unclassified category Alarm** check box to enable the alarms to be generated for unclassified interference category. Cisco CleanAir can detect and monitor unclassified interferences. Unclassified interference are interference that are detected but do not correspond to any of the known interference types. The Unclassified category alarm is generated when the unclassified severity goes above the configured threshold value for unclassified severity or when the air quality index goes below the configured threshold value for Air Quality Index.

– Air Quality Unclassified Category Severity Threshold—If you selected the Air Quality Unclassified category Alarm check box, enter a value between 1 and 99 (inclusive) in the Air Quality Unclassified Severity Threshold text box to specify the threshold at which you want the unclassified category alarm to be triggered. The default is 20.

– Interferers For Security Alarm—Select the **Interferers For Security Alarm** check box to trigger interferer alarms when the controller detects specified device types, or unselect it to disable this feature. The default value is selected.

– Make sure that any sources of interference that need to trigger interferer alarms appear in the Interferers Selected for Security Alarms text box and any that do not need to trigger interferer alarms appear in the Interferers Ignored for Security Alarms text box. Use the > and < buttons to move interference sources between these two text boxes. By default, all interference sources trigger interferer alarms.

– Event Driven RRM—To trigger spectrum event-driven Radio Resource Management (RRM) to run when a CleanAir-enabled access point detects a significant level of interference, use the following parameters:

  – Event Driven RRM—Displays the current status of spectrum event-driven RRM.

  – Sensitivity Threshold—If Event Driven RRM is enabled, this text box displays the threshold level at which event-driven RRM is triggered. It can have a value of either Low, Medium, or High. When the interference for the access point rises above the threshold level, RRM initiates a local Dynamic Channel Allocation (DCA) run and changes the channel of the affected access point radio if possible to improve network performance. Low represents a decreased sensitivity to changes in the environment while High represents an increased sensitivity.

**Step 4** Click **Save**.
Configuring Mesh Parameters

To configure mesh parameters for an individual controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**.

**Step 2** From the left pane, choose **Device Type > Wireless Controller**.

**Step 3** Click the name of the corresponding controller.

**Step 4** From the left pane, choose **Mesh > Mesh Settings**.

**Step 5** View or edit the following mesh parameters:

- **RootAP to MeshAP Range** — By default, this value is 12,000 feet. You can enter a value between 150 and 132,000 feet. Enter the optimum distance (in feet) that exists between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.

- **Client Access on Backhaul Link** — Enabling this feature lets mesh access points associate with 802.11a wireless clients over the 802.11a backhaul. This is in addition to the existing communication on the 802.11a backhaul between the root and mesh access points. This feature is applicable only to the access points with two radios. Changing Backhaul Client Access reboots all the mesh access points. See the “Client Access on 1524SB Dual Backhaul” in the Related Topics for more information.

- **Background Scanning** — Select the **Background Scanning** check box to enable mesh background scanning feature. The default value is disabled.

  The Mesh Background Scanning and Auto parent selection feature enables a mesh access point (MAP) to find and connect with a better potential parent across channels and maintain its uplink with the best parent all the time.

  This feature eliminates the time consuming task of finding a parent across channels by scanning all the channels. The off-channel procedure transmits broadcast packets on selected channels (at a periodicity of 3 seconds, with a maximum of 50 milliseconds per off-channel) and receives packets from all 'reachable' neighbors. This keeps the child MAP updated with neighbor information across channels enabling it to 'switch' to a new neighbor and use it as a parent for the uplink. The 'switch' need not be triggered from parent loss detection, but on identifying a better parent while the child MAP still has its current parent uplink active.

- **Mesh DCA Channels** — Enabling this option lets the backhaul channel to deselect on the controller using the DCA channel list. Any change to the channels in the Controller DCA list is pushed to the associated access points. This option is only applicable for 1524SB mesh access points. See the “Backhaul Channel Deselection in PI” in the Related Topics for more information.

- **Mesh RAP Downlink Backhaul** — Changing backhaul downlink slot reboots all Mesh APs.

- **Outdoor Access For UNII 1 Band Channels**

- **Global Public Safety** — Enabling this option indicates that 4.9 Ghz can be used on backhaul link by selecting channel on the 802.11a backhaul radio. 4.9Ghz considered to be public safety band and is limited to some service providers. This setting applies at the controller level.
• Security Mode—Choose **EAP** (Extensible Authentication Protocol) or **PSK** (Pre-Shared Key) from the Security Mode drop-down list. Changing Security reboots all mesh access points.

**Step 6**
Click **Save**.

---

**Related Topics**
- Client Access on 1524SB Dual Backhaul
- Backhaul Channel Deselection in PI

---

**Client Access on 1524SB Dual Backhaul**

The 1524 Serial Backhaul (SB) access point consists of three radio slots.

- Radio in slot-0 operates in 2.4 GHz frequency band and is used for client access.
- Radios in slot-1 and slot-2 operate in 5.8 GHz band and are primarily used for backhaul.

The two 802.11a backhaul radios use the same MAC address. There might be instances where the same WLAN maps to the same BSSID in more than one slot.

By default, client access is disabled over both the backhaul radios.

The guidelines must be followed to enable or disable a radio slot:

- You can enable client access on slot-1 even if client access on slot-2 is disabled.
- You can enable client access on slot-2 only when client access on slot-1 is enabled.
- If you disable client access on slot-1, then client access on slot-2 is automatically disabled.
- All the Mesh Access Points reboot whenever the client access is enabled or disabled.

The Universal Client Access feature allows client access over both the slot-1 and slot-2 radios. You can configure client access over backhaul radio from either one of the following:

- The Controller command-line interface (CLI)
- The Controller Graphical User Interface (GUI)
- Prime Infrastructure GUI. See the “Configuring Client Access in PI” in the Related Topics for more information.

**Related Topics**
- Configuring Client Access in PI
- Backhaul Channel Deselection in PI
- Configuring Mesh Parameters

---

**Configuring Client Access in PI**

To configure client access on the two backhaul radios, follow these steps:

**Step 1**
Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2**
Click the device name of the applicable controller.

**Step 3**
From the left sidebar menu, choose **Mesh > Mesh Settings**.
Step 4 Select the **Client Access on Backhaul Link** check box.

Step 5 Select the **Extended Backhaul Client Access** check box.

Step 6 Click **Save**.

   A warning message is displayed:

   *Enabling client access on both backhaul slots will use same BSSIDs on both the slots. Changing Backhaul Client Access will reboot all Mesh APs.*

Step 7 Click **OK**.

   The Universal Client access is configured on both the radios.

---

**Related Topics**

- Backhaul Channel Deselection in PI
- Configuring Mesh Parameters
- Client Access on 1524SB Dual Backhaul

---

**Backhaul Channel Deselection in PI**

To configure backhaul channel deselection, follow these steps:

---

**Step 1** Configure the Mesh DCA channels flag on the controllers. See the “Configuring Mesh DCA Channel Flag on Controllers Using PI” for more information.

**Step 2** Change the channel list using configuration groups. See the “Changing the Channel List Using Configuration Groups” for more information.

---

**Related Topics**

- Configuring Mesh DCA Channel Flag on Controllers Using PI
- Changing the Channel List Using Configuration Groups
- Configuring Client Access in PI
- Client Access on 1524SB Dual Backhaul
- Configuring Mesh Parameters

---

**Configuring Mesh DCA Channel Flag on Controllers Using PI**

You can configure the Mesh DCA Channel flag to push each channel change on one or more controllers to all the associated 1524SB access points. To configure this feature, follow these steps:

---

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **Mesh > Mesh Settings**.

**Step 4** Select the **Mesh DCA Channels** check box to enable channel selection. This option is unselected by default.
Now the channel changes in the controllers are pushed to the associated 1524SB access points.

Changing the Channel List Using Configuration Groups

You can use controller configuration groups to configure backhaul channel deselection. You can create a configuration group and add the required controllers to the group and use the Country/DCA tab to select or deselect channels for the controllers in that group.

To configure backhaul channel deselection using configuration groups, follow these steps:

Step 1 Choose Configuration > Controller Configuration Groups.
Step 2 Select a configuration group to view its configuration group details.
Step 3 From the Configuration Group detail page, click the Country/DCA tab.
Step 4 Select or unselect the Update Country/DCA check box.

Related Topics
- Configuring Mesh DCA Channel Flag on Controllers Using PI
- Client Access on 1524SB Dual Backhaul
- Backhaul Channel Deselection in PI
-Configuring Mesh Parameters

Configuring Port Parameters

To configure Port parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click an applicable device.
Step 3 From the left sidebar menu, choose Ports > Port Settings.
Step 4 Click the applicable Port Number to open the Port Settings Details page. The following parameters are displayed:
- General Parameters:
  - Port Number—Read-only.
  - Admin Status—Choose Enabled or Disabled from the drop-down list.
  - Physical Mode—Auto Negotiate (Read-only)
  - Physical Status—Full Duplex 1000 Mbps (Read-only).
  - STP Mode—Choose 802.1D, Fast, or Off.
  - Link Traps—Choose Enabled or Disabled.
  - Power Over Ethernet
  - Multicast Application Mode—Select Enabled or Disabled.
  - Port Mode SFP Type—Read-only
• Spanning Tree Protocol Parameters:
  – Priority—The numerical priority number of the ideal switch.
  – Path Cost—A value (typically based on hop count, media bandwidth, or other measures) assigned by the network administrator and used to determine the most favorable path through an internetwork environment (lower the cost, better the path).

**Step 5**  Click **Save**.

**Related Topics**
- Configuring Mesh Parameters
- Configuring Controller Management Parameters
- Configuring Location Configurations
- Configuring IPv6
- Configuring Proxy Mobile IPv6
- Configuring mDNS
- Configuring Application Visibility and Control Parameters
- Configuring NetFlow

**Configuring Controller Management Parameters**

The following management parameters of the controllers can be configured:

• Trap Receivers
• Trap Control
• Telnet and SSH
• Multiple Syslog servers
• Web Admin
• Local Management Users
• Authentication Priority

**Related Topics**
- Configuring Trap Receivers
- Configuring Trap Control Parameters
- Configuring Telnet SSH Parameters
- Configuring Multiple Syslog Servers
- Configuring Web Admin
- Configuring Local Management Users
- Configuring Authentication Priority
Configuring Trap Receivers

The trap receiver parameter can be configured for individual wireless controllers. This parameter can be added / deleted from the wireless controller. A trap receiver can be added by creating a template under Configuration > Features & Technologies.

Related Topics
- Configuring Trap Receivers for an Individual Controller
- Deleting a Receiver

Configuring Trap Receivers for an Individual Controller

To configure trap receivers for an individual controller, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configuration &gt; Network &gt; Network Devices, then from the Device Groups menu on the left, select Device Type &gt; Wireless Controller.</td>
</tr>
<tr>
<td>2</td>
<td>Click the device name of the applicable controller.</td>
</tr>
<tr>
<td>3</td>
<td>From the left sidebar menu, choose Management &gt; Trap Receiver.</td>
</tr>
</tbody>
</table>
| 4      | The following parameters are displayed for current trap receivers:  
  - Community Name—Name of the trap receiver.  
  - IP Address—The IP address of the server.  
  - Admin Status—Status must be enabled for the SNMP traps to be sent to the receiver. |
| 5      | Click a receiver Name to access its details. |
| 6      | Select the Admin Status check box to enable the trap receiver. Unselect the check box to disable the trap receiver. |
| 7      | Click Save. |

Deleting a Receiver

To delete a receiver / receivers, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select the applicable receiver / receivers check-box.</td>
</tr>
<tr>
<td>2</td>
<td>From the Select a command drop-down list, choose Delete Receivers.</td>
</tr>
<tr>
<td>3</td>
<td>Click Go.</td>
</tr>
<tr>
<td>4</td>
<td>Click OK in the confirmation message.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Trap Receivers
- Configuring Trap Control Parameters
- Configuring Telnet SSH Parameters
- Configuring Multiple Syslog Servers
Configuring Trap Control Parameters

To configure trap control parameters for an individual controller, follow these steps:

**Step 1**  Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2**  Click the device name of the applicable controller.

**Step 3**  From the left sidebar menu, choose **Management > Trap Control**.

**Step 4**  The following traps can be enabled for this controller:

- **Miscellaneous Traps:**
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated. When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure.
  - Link (Port) Up/Down—Link changes status from up or down.
  - Multiple Users—Two users login with the same login ID.
  - Spanning Tree—Spanning Tree traps. See the STP specifications for descriptions of individual parameters.
  - Rogue AP—Whenever a rogue AP is detected this trap is sent with its MAC address; For a rogue AP that was detected earlier and it no longer exists, this trap is sent.
  - Config Save—Notification sent when the controller configuration is modified.
  - RFID Limit Reached Threshold—The maximum permissible value for RFID limit.

- **Client Related Traps:**
  - 802.11 Association—The associate notification is sent when the client sends an association frame.
  - 802.11 Disassociation—The disassociate notification is sent when the client sends a disassociation frame.
  - 802.11 Deauthentication—The deauthenticate notification is sent when the client sends a deauthentication frame.
  - 802.11 Failed Authentication—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'.
  - 802.11 Failed Association—The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'.
  - Excluded—The associate failure notification is sent when a client is excluded.
  - 802.11 Authenticated—The authenticate notification is sent when the client sends an authentication frame with a status code 'successful'.
  - MaxClients Limit Reached Threshold—The maximum permissible number of clients allowed.

- **Cisco AP Traps:**
Configuring Controller Security Parameters

- AP Register—Notification sent when an access point associates or disassociates with the controller.
- AP Interface Up/Down—Notification sent when access point interface (802.11a or 802.11b/g) status goes up or down.

- Auto RF Profile Traps:
  - Load Profile—Notification sent when Load Profile state changes between PASS and FAIL.
  - Noise Profile—Notification sent when Noise Profile state changes between PASS and FAIL.
  - Interference Profile—Notification sent when Interference Profile state changes between PASS and FAIL.
  - Coverage Profile—Notification sent when Coverage Profile state changes between PASS and FAIL.

- Auto RF Update Traps:
  - Channel Update—Notification sent when access point dynamic channel algorithm is updated.
  - Tx Power Update—Notification sent when access point dynamic transmit power algorithm is updated.

- AAA Traps
  - User Auth Failure—This trap is to inform that a client RADIUS Authentication failure has occurred.
  - RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.

- 802.11 Security Traps:
  - WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error.
  - Signature Attack—Notification sent when a signature attack is detected in the wireless controller that uses RADIUS Authentication.

**Step 5** After selecting the applicable parameters, click **Save**.

---

**Related Topics**

- Configuring Trap Receivers
- Configuring Telnet SSH Parameters
- Configuring Multiple Syslog Servers
- Configuring Web Admin
- Configuring Local Management Users
- Configuring Authentication Priority

---

**Configuring Telnet SSH Parameters**

To configure Telnet SSH (Secure Shell) parameters for an individual controller, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

---

**Cisco Prime Infrastructure 3.1.4 User Guide**

27-cxlvii
Step 3  From the left sidebar menu, choose Management > Telnet SSH.

The following parameters can be configured:

- **Session Timeout**—Indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. Might be specified as a number from 0 to 160. The factory default is 5.
- **Maximum Sessions**—From the drop-down list, choose a value from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed.
- **Allow New Telnet Sessions**—Indicates that new Telnet sessions are not allowed on the DS Port when set to no. The factory default value is no. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.
- **Allow New SSH Sessions**—Indicates that new Secure Shell Telnet sessions are not allowed when set to no. The factory default value is yes.

Step 4  After configuring the applicable parameters, click Save.

---

**Related Topics**

- Configuring Trap Receivers
- Configuring Trap Control Parameters
- Configuring Multiple Syslog Servers
- Configuring Web Admin
- Configuring Local Management Users
- Configuring Authentication Priority

---

**Configuring Multiple Syslog Servers**

For Release 5.0.148.0 controllers or later, you can configure multiple (up to three) syslog servers on the WLAN controller. With each message logged, the controller sends a copy of the message to each configured syslog host, provided the message has severity greater than or equal to the configured syslog filter severity level.

To enable syslogs for an individual controller, follow these steps:

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2  Click the device name of the applicable controller.

Step 3  From the left sidebar menu, choose Management > Multiple Syslog.

The applied template is identified:

- **Syslog Server Address**—Indicates the server address of the applicable syslog.

Step 4  Click Save.

---

**Deleting a Syslog Server**

To delete syslog server(s), follow these steps:
Step 1 Select the syslog server(s) check-box.
Step 2 From the Select a command drop-down list, choose Delete Syslog Servers.
Step 3 Click Go.
Step 4 Click OK in the confirmation message.

Related Topics
• Configuring Trap Receivers
• Configuring Trap Control Parameters
• Configuring Telnet SSH Parameters
• Configuring Web Admin
• Configuring Local Management Users
• Configuring Authentication Priority

Configuring Web Admin

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You can download an externally generated certificate.

To enable WEB admin parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 From the left sidebar menu, choose Management > Web Admin.

The following parameters can be configured:
• WEB Mode—Choose Enable or Disable from the drop-down list. When enabled, users can access the controller GUI using http://ip-address. The default is Disabled. Web mode is not a secure connection.
• Secure Web Mode—Choose Enable or Disable from the drop-down list. When enabled, users can access the controller GUI using https://ip-address. The default is Enabled.
• Certificate Type—The Web Admin certificate must be downloaded. The controller must be rebooted for the new Web Admin certificate to take effect.
  • Download Web Admin Certificate—Click to access the Download Web Admin Certificate to Controller page. See “Downloading Web Auth or Web Admin Certificate to the Controller” for more information.

Downloading Web Auth or Web Admin Certificate to the Controller

To download a Web Auth or Web Admin Certificate to the controller, follow these steps:
Step 1   Click the Download Web Admin Certificate or Download Web Auth Certificate link.

Step 2   In the File is located on field, specify Local machine or TFTP server. If the certificate is located on the TFTP server, enter the server filename. If it is located on the local machine, click Browse and enter the local filename.

Step 3   Enter the TFTP server name in the Server Name text box. The default is the Prime Infrastructure server.

Step 4   Enter the server IP address.

Step 5   In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 6   In the Time Out text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 7   In the Local File Name text box, enter the directory path of the certificate.

Step 8   In the Server File Name text box, enter the name of the certificate.

Step 9   Enter the password in the Certificate Password text box.

Step 10  Re-enter the above password in the Confirm Password text box.

Step 11  Click OK.

Step 12  Click Regenerate Cert to regenerate the certificate.

Related Topics

- Configuring Web Admin
- Configuring Trap Receivers
- Configuring Trap Control Parameters
- Configuring Telnet SSH Parameters
- Configuring Multiple Syslog Servers
- Configuring Local Management Users
- Configuring Authentication Priority

Configuring Local Management Users

This page lists the names and access privileges of the local management users. You can also delete the local management user.

To access the Local Management Users page, follow these steps:

Step 1   Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2   Click the device name of the applicable controller.

Step 3   From the left sidebar menu, choose Management > Local Management Users.

Step 4   Click a username.

  - User Name (read-only)—Name of the user.
Access Level (read-only)—Read Write or Read Only.

Deleting the Local Management User

To delete the Local Management User, follow these steps:

- **Step 1**: Select the user(s) check-box.
- **Step 2**: From the **Select a command** drop-list, choose **Delete Local Management Users**.
- **Step 3**: Click **Go**.
- **Step 4**: Click **OK** in the confirmation message.

Related Topics
- Configuring Authentication Priority
- Configuring Trap Receivers
- Configuring Trap Control Parameters
- Configuring Telnet SSH Parameters
- Configuring Multiple Syslog Servers
- Configuring Web Admin

Configuring Authentication Priority

Authentication Priority is configured to control the order in which authentication servers are used to authenticate controller management users.

To access the Authentication Priority page, follow these steps:

- **Step 1**: Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.
- **Step 2**: Click the device name of the applicable controller.
- **Step 3**: From the left sidebar menu, choose **Management > Authentication Priority**.
- **Step 4**: The local database is searched first. Choose either RADIUS or TACACS+ for the next search. If authentication using the local database fails, the controller uses the next type of server.
- **Step 5**: Click **Save**.

Related Topics
- Configuring Controller Management Parameters
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Location Configurations
- Configuring IPv6
Cisco Prime Infrastructure 3.1.4 User Guide

Chapter 27 Configuring Wireless Devices

- Configuring Proxy Mobile IPv6
- Configuring mDNS
- Configuring Application Visibility and Control Parameters
- Configuring NetFlow

Configuring Location Configurations

Currently WiFi clients are moving towards lesser probing to discover an AP. Smartphones do this to conserve battery power. The applications on a smartphone have difficulty generating probe request but can easily generate data packets and hence trigger enhanced location for the application. Hyperlocation is configured from WLC 8.1MR and Prime Infrastructure 3.1. It is ultra-precise in locating beacons, inventory, and personal mobile devices. Some networks use multiple access points to get location coordinates within 5 to 7 meters of accuracy, but Hyperlocation can track locations to within a single meter.

To configure location configurations for an individual controller, follow these steps:

Step 1
Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2
Click the device name of the applicable controller.

Step 3
From the left sidebar menu, choose Location > Location Configuration.

Step 4
Add or modify the General parameters:

- RFID Tag Data Collection—Select the check box to enable the collection of data on tags.

Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command `config rfid status enable` on the controllers.

- Location Path Loss Configuration
  - Calibrating Client—Select the check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrate clients. Packets are transmitted on all channels. All access points gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.
  - Normal Client—Select the check box to have a non-calibrating client. No S36 requests are transmitted to the client. S36 is compatible with CCXv2 or later whereas S60 is compatible with CCXv4 or later.

- Measurement Notification Interval (in secs)
  - Tags, Clients, and Rogue APs/Clients—Allows you to set the NMSP measurement notification interval for clients, tags, and rogues. Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue access points/clients).

Setting this value on the controller generates an out-of-sync notification which you can view in the Synchronize Servers page. When different measurement intervals exist between a controller and the mobility services engine, the largest interval setting of the two is adopted by the mobility services engine.
Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine. Synchronization to the mobility services engine is required if changes are made to measurement notification interval.

- **RSS Expiry Timeout (in secs)**
  - For Clients—Enter the number of seconds after which RSSI measurements for normal (non-calibrating) clients must be discarded.
  - For Calibrating Clients—Enter the number of seconds after which RSSI measurements for calibrating clients must be discarded.
  - For Tags—Enter the number of seconds after which RSSI measurements for tags must be discarded.
  - For Rogue APs—Enter the number of seconds after which RSSI measurements for rogue access points must be discarded.

**Step 5** Add or modify the Advanced parameters:

- **RFID Tag Data Timeout (in secs)**—Enter a value (in seconds) to set the RFID tag data timeout setting.
- **Location Path Loss Configuration**
  - Calibrating Client Multiband—Select the Enable check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled in the general tab as well. To use all radios (802.11a/b/g/n) available, you must enable multiband.
- **Hyperlocation Config Parameters**
  - Hyperlocation—By enabling this option, all the APs associated to that controller which have the Hyperlocation module will be enabled.
  - Packet Detection RSSI Minimum—Adjust this value to filter out weak RSSI readings from location calculation.
  - Scan Count Threshold for Idle Client Detection—The maximum permissible count of the idle clients detected while scanning.
  - NTP Server IP Address—Enter the valid NTP server IP address. This IP address is used by all APs for time synchronization.

**Step 6** Click Save.

---

**Related Topics**

- Configuring IPv6
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Controller Management Parameters
- Configuring Proxy Mobile IPv6
- Configuring mDNS
- Configuring Application Visibility and Control Parameters
- Configuring NetFlow
Configuring IPv6

IPv6 can be configured with Neighbor Binding Timer and Router Advertisements (RA) parameters.

Related Topics
- Configuring Neighbor Binding Timers
- Configuring RA Throttle Policy
- Configuring RA Guard

Configuring Neighbor Binding Timers

To configure the Neighbor Binding Timers, follow these steps:

1. Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
2. Click the device name of the applicable controller.
3. From the left sidebar menu, choose IPv6 > Neighbor Binding Timers.
4. The applied template will be displayed. Add or modify the following parameters:
   - Down Lifetime Interval—This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.
   - Reachable Lifetime Interval—This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.
   - Stale Lifetime Interval—This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.
5. Click Save.

Configuring RA Throttle Policy

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network.

To configure RA Throttle Policy, follow these steps:

1. Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
2. Click the device name of the applicable controller.
3. From the left sidebar menu, choose IPv6 > RA Throttle Policy.
4. If you want to enable the RA Throttle Policy, select the Enable check box and configure the following parameters:
   - Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
   - Max Through—The number of RA that passes through over a period or over an unlimited period. If the No Limit check-box is not enabled, the maximum pass-through number can be specified.
   - Interval Option—Indicates the behavior in case of RA with an interval option.
Configuring RA Guard

RA Guard is a Unified Wireless solution to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can configure IPv6 Router Advertisement parameters.

To configure RA Guard, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **IPv6 > RA Guard**.

**Step 4** If you want to enable the Router Advertisement Guard, select the **Enable** check box.

**Step 5** Click **Save**.

### Related Topics
- Configuring IPv6
- Configuring Proxy Mobile IPv6
- Configuring mDNS
- Configuring Application Visibility and Control Parameters
- Configuring NetFlow
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Controller Management Parameters
- Configuring Location Configurations

---

**Configuring Controller Security Parameters**

- Ignore
- Passthrough
- Throttle

- Allow At-least—Indicates the minimum number of RA not throttled per router.
- Allow At-most—Indicates the maximum or unlimited number of RA not throttled per router. If the **No Limit** check-box is not enabled, the maximum number of RA not throttled per router can be specified.

**Step 5** Click **Save**.

### Related Topics
- Configuring RA Guard
- Configuring Neighbor Binding Timers

---

**Configuring RA Guard**

RA Guard is a Unified Wireless solution to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can configure IPv6 Router Advertisement parameters.

To configure RA Guard, follow these steps:

**Step 1** Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click the device name of the applicable controller.

**Step 3** From the left sidebar menu, choose **IPv6 > RA Guard**.

**Step 4** If you want to enable the Router Advertisement Guard, select the **Enable** check box.

**Step 5** Click **Save**.

### Related Topics
- Configuring IPv6
- Configuring Proxy Mobile IPv6
- Configuring mDNS
- Configuring Application Visibility and Control Parameters
- Configuring NetFlow
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Controller Management Parameters
- Configuring Location Configurations
Configuring Proxy Mobile IPv6

Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node and initiate the mobility signaling and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

Related Topics
- Configuring PMIP Global Configurations
- Configuring LMA Configurations
- Configuring PMIP Profile

Configuring PMIP Global Configurations

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose PMIP > Global Config from the left sidebar menu.

Step 4 Configure the following fields:
- Domain Name—Read-only.
- MAG Name—Read-only.
- MAG Interface—Read-only.
- Maximum Bindings Allowed—Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 to 7000.
- Binding Lifetime—Lifetime of the binding entries in the controller. The valid range is between 10 to 65535 seconds. The default value is 65535. The binding lifetime should be a multiple of 4 seconds.
- Binding Refresh Time—Refresh time of the binding entries in the controller. The valid range is between 4 to 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4 seconds.
- Binding Initial Retry Timeout—Initial timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 1000 second.
- Binding Maximum Retry Timeout—Maximum timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 32000 seconds.
- Replay Protection Timestamp—Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The valid range is between 1 to 255 milliseconds. The default value is 7 milliseconds.
• Minimum BRI Retransmit Timeout—Minimum amount of time that the controller waits before retransmitting the BRI message. The valid range is between 500 to 65535 seconds.
• Maximum BRI Retransmit Timeout—Maximum amount of time that the controller waits before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 to 65535 seconds. The default value is 2000 seconds.
• BRI Retries—Number of BRI retries.
• MAG APN—Name of the Access Point Node of MAG.

Step 5 Click Save.

Related Topics
• Configuring LMA Configurations
• Configuring PMIP Profile
• Configuring Proxy Mobile IPv6

Configuring LMA Configurations

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 Choose PMIP > LMA Config from the left sidebar menu.
Step 4 Configure the following fields:
  • LMA Name—Name of the LMA connected to the controller.
  • LMA IP Address—IP address of the LMA connected to the controller.
Step 5 Click Save.

Deleting LMA Configurations

To delete the LMA configurations, follow these steps:

Step 1 Select the applicable LMA config check-box.
Step 2 From the Select a command drop-list, choose Delete PMIP Local Configs.
Step 3 Click Go.
Step 4 Click OK in the confirmation message.

Related Topics
• Configuring LMA Configurations
• Configuring PMIP Profile
• Configuring Proxy Mobile IPv6
• Configuring Proxy Mobile IPv6

## Configuring PMIP Profile

### Step 1
Choose **Configuration > Network > Network Devices**, then from the **Device Groups** menu on the left, select **Device Type > Wireless Controller**.

### Step 2
Click the device name of the applicable controller.

### Step 3
Choose **PMIP > PMIP Profile** from the left sidebar menu.

### Step 4
Enter the profile name.

### Step 5
Click **Add** and then configure the following fields:

- **Network Access Identifier**—Name of the Network Access Identifier (NAI) associated with the profile.
- **LMA Name**—Name of the LMA to which the profile is associated.
- **Access Point Node**—Name of the access point node connected to the controller.

### Step 6
Click **Save**.

### Related Topics
- Configuring PMIP Global Configurations
- Configuring LMA Configurations
- Configuring Proxy Mobile IPv6

## Deleting PMIP Profiles

To delete the PMIP profiles, follow these steps:

### Step 1
Select the required PMIP profiles check-box.

### Step 2
From the **Select a command** drop-list, choose **Delete PMIP Local Configs**.

### Step 3
Click **Go**.

### Step 4
Click **OK** in the confirmation message.

### Related Topics
- Configuring mDNS
- Configuring EoGRE Tunneling
- Configuring Application Visibility and Control Parameters
- Configuring NetFlow
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Controller Management Parameters
- Configuring Location Configurations
Configuring EoGRE Tunneling

Ethernet over GRE (EoGRE) is a new aggregation solution for aggregating Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. When the IP GRE tunnels are terminated on a service provider broadband network gateway, the end host’s traffic is terminated and subscriber sessions are initiated for the end host.

To configure EoGRE tunneling on Prime Infrastructure, follow these steps:

Step 1: Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2: Click the device name of the applicable controller.

Step 3: Choose Tunneling > EoGRE from the left sidebar menu.

Step 4: From the Interface Name drop-down list, choose the source interface to tunnel.

Step 5: Click Save.

Related Topics
- Configuring mDNS
- Configuring Application Visibility and Control Parameters
- Configuring NetFlow
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Controller Management Parameters
- Configuring Location Configurations
- Configuring IPv6

Configuring mDNS

Multicast DNS (mDNS) service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast and supports zero configuration IP networking. You can configure mDNS so that the controller can learn about the mDNS services and advertise these services to all clients.

There are two tabs in mDNS—Services and Profiles.

- Services tab—This tab enables you to configure the global mDNS parameters and update the Master Services database.
- Profiles tab—This tab enables to view the mDNS profiles configured on the controller and create new mDNS profiles. After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups.
followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority. By default, the controller has an mDNS profile, default-mdns-profile which cannot be deleted.

---

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

**Step 2** Click the device name of the applicable controller.

**Step 3** Choose mDNS > mDNS from the left sidebar menu.

**Step 4** On the Services tab, configure the following parameters:

- **Template Applied**—The name of the template applied to this controller.
- **mDNS Global Snooping**—Check box that you select to enable snooping of mDNS packets. The controller does not support IPv6 mDNS packets even when you enable mDNS snooping.
- **Query Interval (10-120)**—mDNS query interval, in minutes that you can set. This interval is used by WLC to send periodic mDNS query messages to services which do not send service advertisements automatically after they are started. The range is from 10 to 120 minutes. The default value is 15 minutes.
- **Master Services**—Click Add Row and then configure the following fields:
  - **Master Service Name**—Drop-down list from which you can choose the supported services that can be queried. To add a new service, enter or choose the service name, enter the service string, and then choose the service status. The following services are available:
    - AirTunes
    - AirPrint
    - AppleTV
    - HP Photosmart Printer1
    - HP Photosmart Printer2
    - Apple File Sharing Protocol (AFP)
    - Scanner
    - Printer
    - FTP
    - iTunes Music Sharing
    - iTunes Home Sharing
    - iTunes Wireless Device Syncing
    - Apple Remote Desktop
    - Apple CD/DVD Sharing
    - Time Capsule Backup
  - **Master Service Name**—Name of the mDNS service.
  - **Service String**—Unique string associated to an mDNS service. For example, _airplay._tcp.local. is the service string associated to AppleTV.
  - **Query Status**—Check box that you select to enable an mDNS query for a service. Periodic mDNS query messages will be sent by WLC at configured Query Interval for services only when the query status is enabled; otherwise, service should automatically advertised for other services where the query status is disabled (for example AppleTV).
Step 5 On the Profiles tab, configure the following parameters:

- Profiles—Click Add Profile and then configure the following fields:
  - Profile Name—Name of the mDNS profile. You can create a maximum of 16 profiles.
  - Services—Select the services (using the check boxes) that you want to map to the mDNS profile.
- You can edit or delete the existing profile by clicking on Edit and Delete respectively.

Step 6 Click Save.

Configuring mDNS Policies

By default, the controller creates an access policy, default-mdns-policy which cannot be deleted. This is displayed with the Group Name and Description. Select the policy to view its Service Group details. Click Save after editing the fields.

Related Topics
- Configuring Application Visibility and Control Parameters
- Configuring NetFlow
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Controller Management Parameters
- Configuring Location Configurations
- Configuring IPv6
- Configuring Proxy Mobile IPv6

Configuring Application Visibility and Control Parameters

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1400 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, expensive network link usage, and infrastructure upgrades.

AVC is supported only on the Cisco 2500 and 5500 Series Controllers, and Cisco Flex 7500 and Cisco 8500 Series Controllers.

Configuring AVC Profiles

To configure the AVC profile, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.
Step 3 Choose Services > Application Visibility And Control > AVC Profile from the left sidebar menu.

Step 4 Click the AVC Profile Name that you want to configure.

Step 5 To create AVC rules, click Add.

Step 6 Configure the following parameters:

- Application Name—Name of the application.
- Application Group Name—Name of the application group to which the application belongs.
- Action—Drop-down list from which you can choose the following:
  - Drop—Drops the upstream and downstream packets corresponding to the chosen application.
  - Mark—Marks the upstream and downstream packets corresponding to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
  - Rate Limit—If you select Rate Limit as an action, you can specify Average Rate Limit per client and Burst data rate limit. The number of rate limit applications is limited to 3.
    The default action is to permit all applications.
- DSCP—Packet header code that is used to define quality of service across the Internet. The DSCP values are mapped to the following QoS levels:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)—Provides lowest bandwidth for guest services.
  - Custom—Specify the DSCP value. The range is from 0 to 63.
- DSCP Value—This value can be entered only when Custom is chosen from the DSCP drop-down list.
- Avg. Rate Limit (in Kbps)—If you select Rate Limit as an action, you can specify Average Rate Limit per client which is the average bandwidth limit of that application.
- Burst Rate Limit (in Kbps)—If you select Rate Limit as an action, you can specify Burst Rate limit which is the peak limit of that application.

Step 7 Click Save.

Related Topics
- Configuring NetFlow
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Controller Management Parameters
- Configuring Location Configurations
- Configuring IPv6
- Configuring Proxy Mobile IPv6
- Configuring mDNS
Chapter 27  Configuring Wireless Devices

Configuring NetFlow

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing by collecting IP traffic information from network devices. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements.
- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter.

Configuring NetFlow Monitor

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configuration &gt; Network &gt; Network Devices, then from the Device Groups menu on the left, select Device Type &gt; Wireless Controller.</td>
</tr>
<tr>
<td>2</td>
<td>Click the device name of the applicable controller.</td>
</tr>
<tr>
<td>3</td>
<td>Choose NetFlow &gt; Monitor from the left sidebar menu.</td>
</tr>
<tr>
<td>4</td>
<td>Configure the following parameters:</td>
</tr>
<tr>
<td></td>
<td>- Monitor Name—Name of the NetFlow monitor. The monitor name can be up to 127 case-sensitive alphanumeric characters. You can configure only one monitor in the controller.</td>
</tr>
<tr>
<td></td>
<td>- Record Name—Name of the NetFlow record. A NetFlow record in the controller contains the following information about the traffic in a given flow:</td>
</tr>
<tr>
<td></td>
<td>- Client MAC address</td>
</tr>
<tr>
<td></td>
<td>- Client Source IP address</td>
</tr>
<tr>
<td></td>
<td>- WLAN ID</td>
</tr>
<tr>
<td></td>
<td>- Application ID</td>
</tr>
<tr>
<td></td>
<td>- Incoming bytes of data</td>
</tr>
<tr>
<td></td>
<td>- Outgoing bytes of data</td>
</tr>
<tr>
<td></td>
<td>- Incoming Packets</td>
</tr>
<tr>
<td></td>
<td>- Outgoing Packets</td>
</tr>
<tr>
<td></td>
<td>- Incoming DSCP</td>
</tr>
<tr>
<td></td>
<td>- Outgoing DSCP</td>
</tr>
<tr>
<td></td>
<td>- Name of last AP</td>
</tr>
<tr>
<td>5</td>
<td>Exporter Name—Name of the exporter. You can configure only one monitor in the controller.</td>
</tr>
<tr>
<td>6</td>
<td>Exporter IP—IP address of the collector.</td>
</tr>
<tr>
<td>7</td>
<td>Port Number—UDP port through which the NetFlow record is exported from the controller.</td>
</tr>
<tr>
<td>8</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>
Configuring NetFlow Exporter

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2  Click the device name of the applicable controller.

Step 3  Choose NetFlow > Exporter from the left sidebar menu.

Step 4  Configure the following parameters:
- Exporter Name—Name of the exporter.
- Exporter IP —IP address of the exporter.
- Port Number—The UDP port through which the Netflow record is exported.

Related Topics
- Configuring Mesh Parameters
- Configuring Port Parameters
- Configuring Controller Management Parameters
- Configuring Location Configurations
- Configuring IPv6
- Configuring Proxy Mobile IPv6
- Configuring mDNS
- Configuring Application Visibility and Control Parameters

Configuring Third-Party Controllers and Access Points

Prime Infrastructure enables you to add third-party controllers and access points. As part of this feature you can perform the following functions:
- Add third-party controllers to the Prime Infrastructure.
- Monitor the state of the third-party controllers.
- Get inventory information for the third-party controllers and their associated access points.
- Use the background tasks to view the operations status third-party controllers and access points.

Related Topics
- Adding a Third-Party Controller
- Viewing Third-Party Controller Operational Status
- Viewing the Details of Third-Party Access Points
- Removing Third-Party Access Points
- Viewing Third-Party Access Point Operational Status
Adding a Third-Party Controller

To add a third-party controller, follow these steps:

**Step 1**  Choose **Configuration > Network Devices > Third Party Wireless Controller**.

**Step 2**  Click **Add Device**.

**Step 3**  In the Add Device page, enter the required parameters in the following tabs:
- General
- SNMP
- Telnet/SSH
- HTTP/HTTPS
- IPSec

**Step 4**  Click **Add**.

**Related Topics**
- Viewing Third-Party Controller Operational Status
- Viewing the Details of Third-Party Access Points
- Removing Third-Party Access Points
- Viewing Third-Party Access Point Operational Status

Viewing Third-Party Controller Operational Status

To view the Third Party Controller Operational Status page, follow these steps:

**Step 1**  Choose **Administration > Settings > Background Tasks**.

**Step 2**  In this page, perform one of the following:
- Execute the task now.
  Select the **Third Party Controller Operational Status** check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.
- Enable the task.
  Select the **Third Party Controller Operational Status** check box. From the Select a command drop-down list, choose **Enable Tasks**, and click **Go**. The task converts from dimmed to available in the Enabled column.
- Disable the task.
  Select the **Third Party Controller Operational Status** check box. From the Select a command drop-down list, choose **Disable Tasks**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

**Step 3**  To modify the task, click the **Third Party Controller Operational Status** link in the Background Tasks column.
The Third Party Controller Operational Status page displays the following information:

- Last Execution Information
  - Start Time.
  - End Time.
  - Elapsed Time (in seconds) of the task.
  - Result—Success or error.
  - Message—Text message regarding this task.

**Step 4** View or modify the following in the Task Details section:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task. The default is 3 hours.

**Step 5** When finished, click **Save** to confirm task changes.

---

**Related Topics**

- Viewing the Details of Third-Party Access Points
- Adding a Third-Party Controller
- Removing Third-Party Access Points
- Viewing Third-Party Access Point Operational Status

---

**Viewing the Details of Third-Party Access Points**

The third-party access points are discovered when you add a third-party controller.

To view the configurations of a third-party access point, follow these steps:

**Step 1** Choose **Configuration > Network Devices > Third Party Access Points**.

**Step 2** Click the AP Name link to display the details. The General tab for that third-party access point appears.

---

**Related Topics**

- Removing Third-Party Access Points
- Adding a Third-Party Controller
- Viewing Third-Party Controller Operational Status
- Viewing Third-Party Access Point Operational Status

---

**Removing Third-Party Access Points**

To remove third-party access points, follow these steps:

**Step 1** Choose **Configuration > Network Devices > Third Party Access Points**.
**Step 2** Select the check boxes of the access points you want to remove.

**Step 3** Click **Delete**.

**Step 4** A confirmation message appears.

**Step 5** Click **Yes**.

---

**Related Topics**

- Viewing Third-Party Access Point Operational Status
- Adding a Third-Party Controller
- Viewing Third-Party Controller Operational Status
- Viewing the Details of Third-Party Access Points

---

### Viewing Third-Party Access Point Operational Status

To view the Third Party Access Point Operational Status page, follow these steps:

**Step 1** Choose **Administration > Settings > Background Tasks**.

**Step 2** In this page, perform one of the following:

- Execute the task now.
  
  Select the Third Party Access Point Operational Status check box. From the Select a command drop-down list, choose **Execute Now**, and click **Go**. You see the status change in the Enabled column.

- Enable the task.
  
  Select the Third Party Access Point Operational Status check box. From the Select a command drop-down list, choose **Enable Tasks**, and click **Go**. The task converts from dimmed to available in the Enabled column.

- Disable the task.
  
  Select the Third Party Access Point Operational Status check box. From the Select a command drop-down list, choose **Disable Tasks**, and click **Go**. The task is dimmed in the Enabled column after the disabling is complete.

**Step 3** To modify the task, click the Third Party Access Point Operational Status link in the Background Tasks column.

The Third Party Controller Operational Status page displays the following information:

- Last Execution Information
  
  - Start Time.
  
  - End Time.
  
  - Elapsed Time (in seconds) of the task.
  
  - Result—Success or error.
  
  - Message—Text message regarding this task.

**Step 4** View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
Configuring Switches

You can add switches to Prime Infrastructure database to view overall switch health and endpoint monitoring and to perform switchport tracing. The following switches can be configured:

- 3750
- 3560
- 3750E
- 3560E
- 2960.

The switch functionality appears on the configuration menu in Prime Infrastructure however you cannot configure switch features using Prime Infrastructure. You can only configure Prime Infrastructure system.

Prime Infrastructure allows you to do the following:

- Add switches in the Configuration > Network > Network Devices > Device Type > Wireless Controller page and specify CLI and SNMP credentials.
- Add a location-capable switch for tracking wired clients by mobility services engine and Prime Infrastructure in the Configuration > Network > Network Devices > Device Type > Wireless Controller page.
- Monitor Switches by choosing Monitor > Network Devices.
- Run switch-related reports using the Reports menu.

Related Topics
- Features Available by Switch Type
- Adding Switches

Features Available by Switch Type

When you add a switch to Prime Infrastructure, you specify how the switch is to be managed, based on this, Prime Infrastructure determines the features that are available:
• Monitored switches—You can add switches (choose Configuration > Network > Network Devices > Device Type > Wireless Controller) and monitor switch operation (choose Monitor > Network Devices). Each switch counts as a single device against the total device count for your license. If you have unused device counts available in your license engine, you can add a switch to Prime Infrastructure. If you have no remaining device counts available, you cannot add additional switches to Prime Infrastructure.

• Switch Port Tracing (SPT) only switches—Switches perform switch port tracing only. SPT-only switches appear in the Configuration > Network > Network Devices > Device Type > Switches and Hubs page and in inventory reports. Licensing does not apply to SPT switches.

Related Topics
• Viewing Switches
• Viewing Switch Details

Viewing Switches

Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs to see a summary of all switches in the Prime Infrastructure database. Click any column heading to sort the information by that column. You can switch between ascending and descending sort order by clicking the column heading more than once.

Related Topics
• Features Available by Switch Type
• Viewing Switch Details

Viewing Switch Details

Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs to see a summary of all switches in the Prime Infrastructure database. Click a Device Name to see detailed information about that switch.

Related Topics
• Features Available by Switch Type
• Viewing Switches
• Example: Configuring SNMPv3 on Switches

Modifying SNMP Parameters

To modify SNMP parameters for a switch, follow these steps:

Step 1  Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs, then click the checkbox next to the switch for which you want to change SNMP credentials.

Step 2  Click Edit.

Step 3  Modify the necessary SNMP Parameters fields, then click one of the following:
Related Topics
- Features Available by Switch Type
- Viewing Switches
- Viewing Switch Details
- Modifying Telnet/SSH Parameters

Modifying Telnet/SSH Parameters

To modify Telnet or SSH parameters for a switch, follow these steps:

Step 1 Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs, then click the checkbox next to the switch for which you want to change Telnet or SSH credentials.
Step 2 Click Edit.
Step 3 Modify the necessary Telnet/SSH Parameters fields, then click one of the following:
  - Reset to restore the previously saved parameters.
  - Save to save and apply the changes you made.
  - Cancel to exit without saving your changes and return to the previous screen.

Related Topics
- Features Available by Switch Type
- Viewing Switches
- Viewing Switch Details
- Modifying SNMP Parameters

Adding Switches

When you add a switch to the Prime Infrastructure database, by default, Prime Infrastructure verifies the SNMP credentials of the switch. If the device credentials are not correct, you receive an SNMP failure message but the switch is added to the Prime Infrastructure database.

To add a switch to Prime Infrastructure, follow these steps:

Step 1 Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs, then click Add Device.
Step 2 Enter the appropriate information in the fields displayed.
Step 3  Click **Add** to add the switch or click **Cancel** to cancel the operation and return to the list of switches.

**Related Topics**
- Example: Configuring SNMPv3 on Switches
- Importing Switches Using a CSV File
- Configure > Switches > Add Switches

**Example: Configuring SNMPv3 on Switches**

The following is an example for configuring SNMPv3 on the switch:

```
snmp-server view v3default iso included
snmp-server group v3group v3 auth write v3default snmp-server user <username> <v3group> v3 auth <md5 or sha> <authentication password>
```

If the switch has VLANs, you must configure each VLAN, otherwise switch porting tracing fails. The following is an example if the switch has VLANs 1 and 20.

```
snmp-server group v3group v3 auth context vlan-1 write v3default
snmp-server group v3group v3 auth context vlan-20 write v3default
```

When you create SNMP v3 view, make sure you include all of the OIDs.

**Related Topics:**
- Importing Switches Using a CSV File

**Importing Switches Using a CSV File**

You can import switches into the Prime Infrastructure database using a CSV file. The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory.

**Example: Importing Switches Using a CSV File**

The following example shows a sample CSV file.

<table>
<thead>
<tr>
<th>ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries, snmp_timeout, protocol, telnet_username, telnet_password, enable_password, telnet_timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1.1.3, 255.255.255.0, v2, public, , , , , , 3, 10, telnet, cisco, cisco, cisco, 60</td>
</tr>
<tr>
<td>16.1.1.4, 255.255.255.0, v2, public, , , , , , 3, 10, ssh2, cisco, cisco, cisco, 60</td>
</tr>
<tr>
<td>16.1.1.5, 255.255.255.0, v2, public, , , , , , 3, 10, , cisco, cisco, cisco, 60</td>
</tr>
<tr>
<td>16.1.1.6, 255.255.255.0, v2, public, , , , , , 3, 10, telnet, cisco, cisco, cisco, 60</td>
</tr>
<tr>
<td>3.3.3.3, 255.255.255.0, v3, , , , , , 3, 4, HMAC-MD5, default, DES, default, 3, 4</td>
</tr>
<tr>
<td>4.4.4.4, 255.255.255.0, v3, , , , , , 3, 4, telnet, cisco, cisco, cisco, cisco, 60</td>
</tr>
</tbody>
</table>

**Related Topics**
- Example: Configuring SNMPv3 on Switches
- Adding Switches
- CSV File Fields
The fields in the Civic Location pane are populated after the civic information is imported.

---

**Removing Switches**

When you remove a switch from the Prime Infrastructure database, the following functions are performed:

- Inventory information for that switch is removed from the database.
- Alarms for the switch remain in the database with a status of Clear. By default, cleared alarms are not displayed in the Prime Infrastructure interface.
- Saved reports remain in the database even if the switch on which the report was run is removed.

**Related Topics**

- Adding Switches
- Removing a Switch from Prime Infrastructure

**Removing a Switch from Prime Infrastructure**

To remove a switch from Prime Infrastructure, follow these steps:

1. Choose **Configuration > Network > Network Devices > Device Type > Switches and Hubs**, then click the checkbox next to the switch for which you want to remove.
2. Click **Delete**.
3. Click **OK** to confirm the deletion.

**Related Topics**

- Adding Switches

---

**Enabling Traps and Syslogs on Switches for Wired Client Discovery**

This section describes how to configure switches to send traps and syslogs to Prime Infrastructure to discover the clients as they connect/disconnect.

**Example: MAC Notification for Traps (Used for Non-Identity Client Discovery)**

The following Cisco IOS configuration example shows how this Cisco IOS switch feature forwards SNMP traps from the switch to Prime Infrastructure server for MAC notifications (for on-802.1x clients):

```
snmp-server enable traps mac-notification change move threshold
```
Enabling Traps and Syslogs on Switches for Wired Client Discovery

```
snmp-server host<IP address of Prime Infrastructure server> version 2c <community-string>
mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change

interface <interface>
  description non-identity clients
  switchport access vlan <VLAN ID>
  switchport mode access
  snmp trap mac-notification change added <- interface level config for MAC Notification
  snmp trap mac-notification change removed <- interface level config for MAC Notification

The debug command is:
  debug snmp packets

The show command is:
  show mac address-table notification change
```

Related Topics
- Configuring MAC Change Notification Traps

Syslog Configuration

The syslog configuration forwards syslog messages from a Catalyst switch to the Prime Infrastructure server. This feature is used for identity clients discovery.

Example: Cisco IOS configuration

```
archive
  log config
    notify syslog contenttype plaintext
  logging facility auth
  logging <IP address of Prime Infrastructure server>
```

Related Topics
- Configuring System Message Logging

OfficeExtend Access Point

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to the residence of an employee. The experience of a teleworker at the home office is exactly the same as it is at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Figure 27-5 illustrates a typical OfficeExtend access point setup.
Enabling Traps and Syslogs on Switches for Wired Client Discovery

Chapter 27      Configuring Wireless Devices

Figure 27-5      Typical OfficeExtend Access Point Setup

OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), thereby enabling an entire group of computers to be represented by a single IP address. In controller release 6.0, only one OfficeExtend access point can be deployed behind a single NAT device.

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a WPlus license can be configured to operate as OfficeExtend access points.

Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

Licensing for an OfficeExtend Access Point

Make sure that the WPlus license is installed on the 5500 series controller. After the license is installed, you can enable the OfficeExtend mode on a 1130 series or 1140 series access point.

The operating system software automatically detects and adds an access point to the Prime Infrastructure database as it associates with existing controllers in the Prime Infrastructure database.

Link Latency Settings for Access Points

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to a controller but is especially useful for FlexConnect access points, for which the link could be a slow or unreliable WAN connection.

Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo requests received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.
The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

Related Topic
- Configuring Link Latency

Configuring Link Latency

To configure link latency, follow these steps:

---

**Step 1** Choose Configuration > Network > Network Devices > Device Type > Unified AP, then click on a Device Name.

**Step 2** Select the Enable Link Latency check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

**Step 3** Click Save to save your changes.

The link latency results appear below the Enable Link Latency check box:

- **Current**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Minimum**—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Maximum**—Because the link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

**Step 4** To clear the current, minimum, and maximum link latency statistics on the controller for this access point, click Reset Link Latency. The updated statistics appear in the Minimum and Maximum fields.

---

Configuring Unified Access Points

You can use the Configuration > Network > Network Devices > Device Type > Unified AP page to view and configure unified access points.

---

**Step 1** Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Unified AP.

**Step 2** Click an applicable IP address to view the following parameters:

- **AP Name**—Click an access point name to view or configure access point details.
- **Base Radio MAC**
- **Admin Status**
- **AP Mode**
- **Software Version**
- **Primary Controller Name**
Step 3 Click an access point name to view or configure the access point details. The displayed information might vary depending for the access point type.

Using the Sniffer Feature

When the sniffer feature is enabled on an access point, the access point functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. The packets contain information on timestamp, signal strength, packet size, and so on.

The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com/products/airopeek/overview

Prerequisites for using the Sniffer Feature

Before using the sniffer feature, you must complete the following:

- Configure an access point in sniffer mode at the remote site. For information on how to configure an access point in sniffer mode, see Configuring an AP in Sniffer Mode Using the Web User Interface in Related Topics.
- Install AiroPeek Version 2.05 or later on a Windows XP machine.
  - You must be a WildPackets Maintenance Member to download the following dll files. See the following URL:
    https://wpdn.wildpackets.com/view_submission.php?id=30
- Copy the following dll files:
  - socket.dll file to the Plugins folder (Example: C:\ProgramFiles\WildPackets\AiroPeek\Plugins)
  - socketres.dll file to the PluginRes folder
    (Example: C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes)

Related Topic
- 802.11 Parameters

Configuring AiroPeek on the Remote Machine

To configure AiroPeek on the remote machine, follow these steps:

Step 1 Start the AiroPeek application and click Options on the Tools tab.
Step 2 Click Analysis Module in the Options page.
Step 3 Right-click inside the page and select Disable All option.
Step 4 Find the Cisco remote module column and enable it. Click OK to save the changes.
Step 5 Click New capture to bring up the capture option page.
Step 6 Choose the remote Cisco adapter and from the list of adapter modules.
Step 7 Expand it to locate the new remote adapter option. Double-click it to open a new page, enter a name in the text box provided and enter the controller management interface IP in the IP address column.
Step 8: Click OK. The new adapter is added to the remote Cisco adapter.

Step 9: Select the new adapter for remote airopeek capture using the access point.

Step 10: Click start socket capture in the capture page to start the remote capture process.

Step 11: From the controller CLI, bring up an access point, and set it to sniffer mode by entering the `config ap mode sniffer ap-name` command.

The access point reboots and comes up in sniffer mode.

---

**Configuring an AP in Sniffer Mode Using the Web User Interface**

To configure an AP in Sniffer mode using the web user interface, follow these steps:

**Step 1**: Choose Configuration > Network > Network Devices, then click an item in the AP Name column to navigate to this page.

**Step 2**: In the General group box, set the AP mode to Sniffer using the drop-down list, and click Apply.

**Step 3**: Click a protocol (802.11a/802.11b/g) in the Protocol column in the Radio Interfaces group box. This opens the configuration page.

**Step 4**: Select the Sniff check box to bring up the Sniff parameters. Select the channel to be sniffed and enter the IP address of the server (The remote machine running AiroPeek).

**Step 5**: Click Save to save the changes.

---

**Configuring Controller Redundancy**

“Controller Redundancy” refers to the High Availability (HA) framework embedded in controllers. Redundancy in wireless network controllers allows you to reduce network downtime. In a redundancy architecture, one controller is in the Active state and a second controller is in the Standby state. The Standby controller monitors the health of the Active controller continuously, using a redundant port. Both controllers share the same configurations including the IP address of the management interface.

The Standby or Active state of a controller is based on the redundancy stock keeping unit (SKU), which is a manufacturing-ordered unique device identifier (UDI). A controller with a redundancy SKU UDI is in the Standby state for the first time when it boots and pairs with a controller that runs a permanent count license. For controllers that have permanent count licenses, you can manually configure whether the controller is in the Active state or the Standby state.

Prime Infrastructure supports stateful switchover of access points (also known as “AP SSO”). AP SSO ensures that AP sessions remain intact despite controller switchovers. For more details on controller redundancy, see “Configuring Wireless Redundancy” in Related Topics.

Controller redundancy is similar to, but separate from, the Prime Infrastructure HA framework used to reduce Prime Infrastructure server downtime. For more information on this, see “Configuring High Availability” in Related Topics.

**Related Topics**

- Configuring High Availability
- Configuring Wireless Redundancy
Configuring Cisco Adaptive wIPS Profiles

Prime Infrastructure supports Cisco Adaptive Wireless Intrusion Prevention System (Cisco Adaptive wIPS, or wIPS), which uses profiles to quickly activate wireless threat protection features.

Prime Infrastructure provides a list of pre-defined wIPS profiles based on customer types, building types, and industry types, such as “Education”, “Financial”, “Military”, “Tradeshow”, and so on. You can use these profiles “as is” or customize them to better meet your needs. You can then apply them to the Mobility Services Engines and controllers you select.

Cisco Adaptive wIPS does not support the Prime Infrastructure partitioning feature.

Related Topics
- Accessing wIPS Profiles
- Adding wIPS Profiles
- Editing wIPS Profiles
- Applying wIPS Profiles
- Deleting wIPS Profiles
- wIPS Policy Alarm Encyclopedia

Accessing wIPS Profiles

Prime Infrastructure’s wIPS Profiles List page provides access to wIPS profiles. You can use it to view, edit, apply or delete current wIPS profiles, and to create new wIPS profiles.

---

**Step 1** Choose Services > Mobility Services > wIPS Profiles. The wIPS Profiles List displays the list of current wIPS profiles. It gives the following information for each existing profile:

- Profile Name—The user-defined name for the wIPS profile.
  To view or edit a wIPS profile, click the Profile Name. Then follow the steps in “Editing wIPS Profiles” in Related Topics
- Profile ID—The profile’s unique identifier.
- Version—The version of the profile.
- MSE(s) Applied To—Indicates the number of Mobility Services Engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- Controller(s) Applied To—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

---

Related Topics
- Configuring Cisco Adaptive wIPS Profiles
- Adding wIPS Profiles
- Editing wIPS Profiles
- Applying wIPS Profiles
- Deleting wIPS Profiles
Creating SSID Groups

Adding wIPS Profiles

You can create new wIPS profiles using the default profile or any of the currently pre-configured profile.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select Services &gt; Mobility Services &gt; wIPS Profiles.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Choose Select a command &gt; Add Profile &gt; Go.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Type a profile name in the Profile Name text box of the Profile Parameters page.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the applicable pre-defined profile, or choose Default from the drop-down list. Pre-defined profiles include the following:</td>
</tr>
<tr>
<td></td>
<td>• Education</td>
</tr>
<tr>
<td></td>
<td>• EnterpriseBest</td>
</tr>
<tr>
<td></td>
<td>• EnterpriseRogue</td>
</tr>
<tr>
<td></td>
<td>• Financial</td>
</tr>
<tr>
<td></td>
<td>• HealthCare</td>
</tr>
<tr>
<td></td>
<td>• HotSpotOpen</td>
</tr>
<tr>
<td></td>
<td>• Hotspot8021x</td>
</tr>
<tr>
<td></td>
<td>• Military</td>
</tr>
<tr>
<td></td>
<td>• Retail</td>
</tr>
<tr>
<td></td>
<td>• Tradeshow</td>
</tr>
<tr>
<td></td>
<td>• Warehouse</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click:</td>
</tr>
<tr>
<td></td>
<td>• Save to save the wIPS profile with no changes and no assignments. The profile appears in the profile list. You can access the profile for edits and assignment later, as explained in “Accessing wIPS Profiles” in Related Topics.</td>
</tr>
<tr>
<td></td>
<td>• Save and Edit to save the profile, edit its settings, and assign it to Mobility Services Engines and Controllers. For details, see “Editing wIPS Profiles” in Related Topics.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Cisco Adaptive wIPS Profiles
- Accessing wIPS Profiles
- Editing wIPS Profiles

Editing wIPS Profiles

The wIPS profile editor allows you to configure profile details, including the following:
- SSID groups—Select the SSID groups to which the wIPS profile will be applied.
- Policy inclusion—Determine which policies are included in the profile.
Configuring Cisco Adaptive wIPS Profiles

Step 1  Access the wIPS profile editor by:
- Create a new wIPS profile and then click **Save and Edit**.
- Choose **Services > Mobility Services > wIPS Profiles** and then click the Profile Name of the wIPS profile you want to edit.

Prime Infrastructure displays the SSID Group List page. Using this page, you can edit and delete current SSID groups or add a new group. You can also select from the global list of SSID groups. For details, see “Associating SSID Groups With wIPS Profiles” in Related Topics.

Step 2  Select the SSID groups you want to associate with the wIPS profile, then click **Save**.

Step 3  Click Next. The Profile Configuration page displays.

Step 4  In the Select Policy pane’s policy tree, select the check boxes of the policies you want to enable or disable in the current profile.

You can enable or disable an entire branch or an individual policy by selecting the check box for the applicable branch or policy.

By default, all policies are selected.

Step 5  In the Profile Configuration page, click an individual policy to display the policy description and to view or modify current policy rule settings. The following options are available for each policy:
- Add—Click **Add** to access the Policy Rule Configuration page to create a new rule for this policy.
- Edit—Select the check box of the applicable rule, and click **Edit** to access the Policy Rule Configuration page to edit the settings for this rule.
- Delete—Select the check box of the rule you want to delete, and click **Delete**. Click **OK** to confirm the deletion.

There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.
- Move Up—Select the check box of the rule you want to move up in the list. Click **Move Up**.
- Move Down—Select the check box of the rule you want to move down in the list. Click **Move Down**.

The following settings can be configured at the policy level:
- Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.

Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues.

Threshold options vary based on the selected policy.

Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page. Choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.
- Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.
- Notification—Indicates the type of notification associated with the threshold.
• ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is be applied.
  Only selected groups trigger the policy.

Step 6  When the profile configuration is complete, click Save to save your changes to the profile.

Step 7  Click Next to display the MSE/Controller(s) page.

Step 8  In the Apply Profile page, select the check boxes of the MSEs and controllers to which you want to apply
  the current profile.

Step 9  When you are finished, click Apply to apply the current profile to the selected MSEs and controllers.
  You can also apply a newly created profile directly from the Profile List page. See “Applying wIPS
  Profiles” in Related Topics.

Related Topics
• Configuring Cisco Adaptive wIPS Profiles
• Applying wIPS Profiles
• Associating SSID Groups With wIPS Profiles
• Configuring Cisco Adaptive wIPS Profiles
• Creating SSID Groups

Applying wIPS Profiles

Step 1  Choose Services > Mobility Services > wIPS Profiles.

Step 2  Select the check boxes of the wIPS profiles you want to apply.

Step 3  Choose Select a command > Apply Profile > Go.

Step 4  Select the mobility services engines and controllers to which you want the profile applied.
  If the new profile assignment is different from the current assignment, you are prompted to save the
  profile with a different name.

Step 5  Click Apply.

Related Topics
• Configuring Cisco Adaptive wIPS Profiles
• Creating SSID Groups

Deleting wIPS Profiles

Profiles currently applied to MSEs and controllers cannot be deleted.

Step 1  Choose Services > Mobility Services > wIPS Profiles.

Step 2  Select the check boxes of the wIPS profiles you want to delete.

Step 3  Choose Select a command > Delete Profile > Go.
Step 4 Click OK to confirm the deletion.

Related Topics
- Configuring Cisco Adaptive wIPS Profiles
- Editing wIPS Profiles
- Associating SSID Groups With wIPS Profiles

Associating SSID Groups With wIPS Profiles

The SSID (Service Set IDentifier) is a token or key which identifies an 802.11 (Wi-Fi) network. Users must either know or be able to discover the SSID to join an 802.11 network.

You can associate SSIDs with a wIPS profile by adding the SSIDs to an SSID group, then associating the SSID group with the wIPS profile.

Related Topics
- Configuring Cisco Adaptive wIPS Profiles
- Creating SSID Groups
- Editing SSID Groups
- Deleting SSID Groups

Creating SSID Groups

Step 1 Choose Services > Mobility Services > wIPS Profiles.
Step 2 Click the Profile Name of any wIPS profile. Prime Infrastructure displays the SSID Group List page.
Step 3 Choose Select a command > Add Group > Go.
Step 4 Enter the SSID Group Name in the text box.
Step 5 Enter the SSIDs in the SSID List text box. Enter multiple SSIDs with a carriage return after each SSID.
Step 6 Click Save.

Related Topics
- Associating SSID Groups With wIPS Profiles
- Configuring Cisco Adaptive wIPS Profiles

Editing SSID Groups

Step 1 Choose Services > Mobility Services > wIPS Profiles.
Step 2 Click the Profile Name of any wIPS profile. Prime Infrastructure displays the SSID Group List page.
Step 3 Select the check box of the SSID group that you want to edit.
Step 4  Choose Select a command > e Edit Group > Go.
Step 5  Make the necessary changes to the SSID Group Name or the SSID List.
Step 6  Click Save.

Related Topics
- Associating SSID Groups With wIPS Profiles
- Configuring Cisco Adaptive wIPS Profiles

Deleting SSID Groups

Step 1  Choose Services > Mobility Services > wIPS Profiles.
Step 2  Click the Profile Name of any wIPS profile. Prime Infrastructure displays the SSID Group List page.
Step 3  Select the check boxes of the SSID groups that you want to delete.
Step 4  Choose Select a command > Delete Group > Go.
Step 5  Click OK to confirm the deletion.

Related Topics
- Associating SSID Groups With wIPS Profiles
- Configuring Cisco Adaptive wIPS Profiles

Managing MSE High Availability Using Prime Infrastructure

You can use Prime Infrastructure to pair and manage Cisco Mobility Services Engine (MSE) devices that have been configured for MSE High Availability (HA). The following related topics explain how to perform these and related tasks.

Related Topics
- Adding MSEs to Prime Infrastructure
- MSE HA Automatic vs Manual Failover and Failback
- Pairing MSE HA Servers
- Viewing Configured Parameters for MSE HA Devices
- Viewing MSE High Availability Status
- Triggering MSE HA Manual Failover or Failback
- Enabling Automatic MSE HA Failover and Failback
MSE HA Automatic vs Manual Failover and Failback

The MSE HA feature is intended to permit continued access to MSE services even when the primary MSE fails. The secondary MSE maintains a complete copy of the primary MSE’s data, serving as its backup. Health Monitor and “heartbeat” processes running on both the primary and secondary keep each server informed about the state of the other.

Whenever the primary MSE fails, a “failover” to the secondary MSE is triggered. Prime Infrastructure will then use the secondary’s mobility services instead of the primary until the problems with the primary are fixed.

When the primary is back in service, a “failback” is triggered, returning control to the primary MSE, and replicating data about the intervening state of the network back to the primary from the secondary MSE.

When configuring MSE HA, you can choose to have failovers triggered either automatically or manually. You have the same options for failbacks.

Configuring MSE HA for manual failover or failback means these operations must be triggered by a user, in response to critical alarms sent when the primary fails or is restored to service.

Configuring MSE HA for automatic failover reduces the need for network administrators to manage MSE HA. It also reduces the time taken to respond to the conditions that provoked the failover, since it brings up the secondary server automatically, within approximately 10 seconds (the default) of detection of failure on the primary. If MSE HA is configured for automatic failback, the system will trigger the failback only after successful receipt of 30 ping messages sent once per minute.

Related Topics
- Pairing MSE HA Servers
- Enabling Automatic MSE HA Failover and Failback
- Managing MSE High Availability Using Prime Infrastructure

Pairing MSE HA Servers

In order to activate High Availability for MSE devices, you must create a pairing, where one MSE serves as the primary MSE device, and another acts as the secondary MSE.

Before You Begin

To create the pairing, you will need to know:

- The device name of the primary MSE server.
- The device name of the secondary MSE server. This can be a previously assigned device name, or a new name you assign at the moment you pair the servers.
- The secondary MSE HA server’s IP address. This is the IP address of the HA Health Monitor, which was assigned when configuring the MSE server for HA use.
- The secondary MSE HA server’s password. This is the Prime Infrastructure communication password, which was assigned when configuring the MSE server for HA use.

Note that you can only pair MSE devices that are:

- Properly configured for use with MSE High Availability, as explained in the related topic “Configuring MSE High Availability”.
- Added to Prime Infrastructure, as explained in the related topic “Adding MSEs to Prime Infrastructure”.
You must also decide if you want to configure the MSE HA servers for manual or automatic failback. For guidelines, see the related topic “MSE HA Automatic vs Manual Failover and Failback”.

**Step 1** Choose **Services > Mobility Services > Mobility Services Engines**. A list of the existing MSEs is displayed.

**Step 2** In the list, find the MSE you want to act as the primary MSE HA server.

**Step 3** The “Secondary Server” column for the MSE listing displays the message “N/A (Click here to configure)”. Click on the link to display the HA configuration page for the primary MSE.

**Step 4** Enter the secondary MSE’s device name, Health Monitor IP address, and Prime Infrastructure communication password in the appropriate fields.

**Step 5** Specify the failover and failback types. You can choose either **Manual** or **Automatic**.

**Step 6** Specify the Long Failover Wait. This is the maximum time the system will wait to trigger automatic failover after detection of primary MSE failure. The default is 10 seconds; the maximum is 120 seconds.

**Step 7** Click **Save**. Prime Infrastructure prompts you to confirm that you want to pair these MSEs. Click OK to confirm.

Prime Infrastructure conducts the pairing and synchronization automatically. These processes can take up to 20 minutes to complete, depending on network bandwidth and many other factors. To check on the progress of these processes, select **Services > Mobility Services Engine > System > Services High Availability > HA Status**.

**Related Topics**
- Configuring MSE High Availability
- Adding MSEs to Prime Infrastructure
- MSE HA Automatic vs Manual Failover and Failback
- Enabling Automatic MSE HA Failover and Failback
- Managing MSE High Availability Using Prime Infrastructure

### Viewing Configured Parameters for MSE HA Devices

**Step 1** Choose **Services > Mobility Services > Mobility Services Engines**.

**Step 2** To see the HA parameters for the:
- Primary MSE HA server: Click the name of the server in the **Device Name** column.
- Secondary MSE HA server: Click the name of the server in the **Secondary Server** column.

Prime Infrastructure displays the Mobility Services Engines configuration page for the server you selected.

**Step 3** In the left sidebar menu, choose **HA Configuration**. The HA Configuration page provides the following information:
- Primary Health Monitor IP
- Secondary Device Name
- Secondary IP Address
Chapter 27  Configuring Wireless Devices

Managing MSE High Availability Using Prime Infrastructure

- Secondary Password
- Secondary Platform UDI
- Secondary Activation Status
- Failover Type
- Failback Type
- Long Failover Wait

Related Topics
- Pairing MSE HA Servers
- Viewing MSE High Availability Status
- Triggering MSE HA Manual Failover or Failback
- Enabling Automatic MSE HA Failover and Failback
- Managing MSE High Availability Using Prime Infrastructure

Viewing MSE High Availability Status

Step 1  Choose Services > Mobility Services > Mobility Services Engines.

Step 2  To see the HA status of the:
- Primary MSE HA server: Click the name of the server in the Device Name column.
- Secondary MSE HA server: Click the name of the server in the Secondary Server column.

Prime Infrastructure displays the Mobility Services Engines configuration page for the server you selected.

Step 3  In the left sidebar menu, choose HA Status. The Current High Availability Status page shows the following information:
- Status—Shows whether the MSE HA server is active and correctly synchronized.
- Heartbeats—Shows whether the MSE HA server is exchanging heartbeat signals with its partner.
- Data Replication—Shows whether MSE HA server is replicating data with its partner.
- Mean Heartbeat Response Time—Shows the mean heartbeat response time between servers.
- Events Log—Shows the last 20 events that the MSE server has generated.

Step 4  Click Refresh Status to update the MSA server’s HA status information and Events Log.

Related Topics
- Pairing MSE HA Servers
- Viewing Configured Parameters for MSE HA Devices
- Enabling Automatic MSE HA Failover and Failback
- Managing MSE High Availability Using Prime Infrastructure
Triggering MSE HA Manual Failover or Failback

Manual failover and failback are enabled by default. Manual configuration requires that the Prime Infrastructure administrator trigger failovers and failbacks manually, in response to system alarms. You can also configure paired MSE HA servers for automatic failover and failback (see Related Topics).

| Step 1 | Choose Services > Mobility Services > Mobility Services Engines. |
| Step 2 | To trigger a: |
| | • Failover from the primary to the secondary: Click the name of the primary MSE HA server in the Device Name column. |
| | • Failback from the secondary to the primary: Click the name of the secondary MSE HA server in the Secondary Server column. |
| | Prime Infrastructure displays the Mobility Services Engines configuration page for the server you selected. |
| Step 3 | In the left sidebar menu, choose HA Configuration. The HA Configuration page displays the HA configuration information for the server you chose. |
| Step 4 | Click Switchover to initiate the failover or failback. |
| Step 5 | Click OK to confirm that you want to initiate the switchover. |

Related Topics

• MSE HA Automatic vs Manual Failover and Failback
• Enabling Automatic MSE HA Failover and Failback
• Managing MSE High Availability Using Prime Infrastructure

Enabling Automatic MSE HA Failover and Failback

Manual failover and failback are enabled by default. If you configure paired MSE HA servers for automatic failover and failback, the change will occur automatically, as follows:

• Failover from primary to secondary: Triggered immediately, as soon as the secondary detects a failure on the primary.
• Failback from secondary to primary: Triggered after 30 successful ping messages from the secondary to the primary. Ping requests are sent once per minute.

| Step 1 | Choose Services > Mobility Services > MSE High Availability. |
| Step 2 | Click the name of the primary MSE HA server in the Device Name column. |
| | Prime Infrastructure displays the HA Configuration page for the primary MSE HA server. |
| Step 3 | In the Failover Type and Failback Type list boxes, select Automatic. |
| Step 4 | If needed: Change the value in Long Failover Wait to control the maximum delay between detection of a failure on the primary and automatic failover. The default is 10 seconds. |
Auto Provisioning for Controllers

Auto provisioning allows Prime Infrastructure to automatically configure a new or replace a current wireless LAN controller (WLC). Prime Infrastructure auto provisioning feature can simplify deployments for customers with a large number of controllers.

For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status.

To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration Settings > Users, Roles, and AAA > User Groups > group name > List of Tasks Permitted in Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

A controller radio and b/g networks are initially disabled by the Prime Infrastructure downloaded startup configuration file. If desired, you might turn on those radio networks by using a template, which should be included as one of the automated templates.

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To access the Auto Provisioning feature, choose Configuration > Plug and Play > WLC Auto Provisioning >.
Creating Controller Configuration Groups

This chapter describes how to create controller configuration groups and mobility groups.

- Adding Controller Configuration Groups
- Configuring Controller Configuration Groups
- Adding or Removing Controllers from a Configuration Group
- Adding or Removing Templates from the Configuration Group
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
- Rebooting Configuration Groups
- About Mobility
- About Mobility Groups
- Mobility Anchors

Adding Controller Configuration Groups

To add new controller configuration groups, follow these steps:

Step 1  Choose Configuration > Templates > Controller Configuration Groups.

Step 2  From the Select a command drop-down list, choose Add Configuration Group, and click Go. The Add New Group page appears.

Step 3  Enter the new configuration group name. It must be unique across all groups.

Step 4  Other templates created in Prime Infrastructure can be assigned to a configuration group. The same WLAN template can be assigned to more than one configuration group. Choose from the following:

- Click Select and add later to add a template at a later time.
- Click Copy templates from a controller to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new configuration group. Only the templates are copied.

The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.
Step 5  Click Save. The Configuration Groups page appears.

Related Topics
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
- Rebooting Configuration Groups
- Configuring Controller Mobility Groups: Workflow
- Configuring Controller Configuration Groups
- Adding or Removing Controllers from a Configuration Group
- Adding or Removing Templates from the Configuration Group
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
- Rebooting Configuration Groups

Configuring Controller Configuration Groups

To configure a controller configuration group, follow these steps:

Step 1  Choose Configuration > Templates > Controller Configuration Groups, and click a group name in the Group Name column. The Configuration Group page appears.

Step 2  Click the General tab. The following options for the configuration group appear:
- Group Name: Name of the configuration group
  - Enable Background Audit—If selected, all the templates that are part of this group are audited against the controller during network and controller audits.
  - Enable Enforcement—If selected, the templates are automatically applied during the audit if any discrepancies are found.

The audit and enforcement of the configuration group template happens when the selected audit mode is Template based audit.
  - Enable Mobility Group—If selected, the mobility group name is pushed to all controllers in the group.
- Mobility Group Name: Mobility Group Name that is pushed to all controllers in the group. The Mobility Group Name can also be modified here. A controller can be part of multiple configuration groups.
- Last Modified On: Date and time configuration group was last modified.
- Last Applied On: Date and time last changes were applied.

Step 3  You must click the Apply/Schedule tab to distribute the specified mobility group name to the group controllers and to create mobility group members on each of the group controllers.

Step 4  Click Save.
Adding or Removing Controllers from a Configuration Group

To add or remove controllers from a configuration group, follow these steps:

**Step 1** Choose Configuration > Templates > Controller Configuration Groups, and click a group name in the Group Name column.

**Step 2** Click the Controllers tab. The columns in the table display the IP address of the controller, the configuration group name the controller belongs to, and the mobility group name of the controller.

**Step 3** Click to highlight the row of the controller you want to add to the group.

**Step 4** Click Add.
If you want to remove a controller from the group, highlight the controller in the Group Controllers box and click Remove.

**Step 5** You must click the Apply/Schedule tab, and click Apply to add or remove the controllers to the configuration groups.

**Step 6** Click Save Selection.

Related Topics
- Adding Controller Configuration Groups
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
- Rebooting Configuration Groups
- Configuring Controller Mobility Groups: Workflow
- Adding Controller Configuration Groups
- Adding or Removing Controllers from a Configuration Group
- Adding or Removing Templates from the Configuration Group
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
- Rebooting Configuration Groups
• Auditing Configuration Groups
• Rebooting Configuration Groups

Adding or Removing Templates from the Configuration Group

To add or remove templates from the configuration group, follow these steps:

**Step 1** Choose Configuration > Templates > Controller Configuration Groups, and click a group name in the Group Name column.

**Step 2** Click the Templates tab. The Remaining Templates table displays the item number of all available templates, the template name, and the type and use of the template.

**Step 3** Click to highlight the row of the template you want to add to the group.

**Step 4** Click Add to move the highlighted template to the Group Templates column. If you want to remove a template from the group, highlight the template in the Remaining Templates box, and click Remove.

**Step 5** You must click the Apply/Schedule tab, and click Apply to add or remove the templates to the configuration groups.

**Step 6** Click Save Selection.

Related topics
• Configuring Controller Mobility Groups: Workflow
• Adding Controller Configuration Groups
• Configuring Controller Configuration Groups
• Adding or Removing Controllers from a Configuration Group
• Applying or Scheduling Configuration Groups
• Auditing Configuration Groups
• Rebooting Configuration Groups

Applying or Scheduling Configuration Groups

The scheduling function allows you to schedule a start day and time for provisioning. Make sure that any other configuration group functions are not performed during the apply provisioning.

To apply the mobility groups, mobility members, and templates to all the controllers in a configuration group, follow these steps:

**Step 1** Choose Configuration > Templates > Controller Configuration Groups, and click a group name in the Group Name column.

**Step 2** Click the Apply/Schedule tab to access this page.
Click **Apply** to start the provisioning of mobility groups, mobility members, and templates to all the controllers in the configuration group. After you apply, you can leave this page or log out of Prime Infrastructure. The process continues, and you can return later to this page to view a report.

A report is generated and appears in the Recent Apply Report page. It shows which mobility group, mobility member, or template were successfully applied to each of the controllers.

If you want to print the report as shown on the page, you must choose landscape page orientation.

**Step 4** Enter a starting date in the text box or use the calendar icon to choose a start date.

**Step 5** Choose the starting time using the hours and minutes drop-down lists.

**Step 6** Click **Schedule** to start the provisioning at the scheduled time.

---

**Related topics**

- Configuring Controller Mobility Groups: Workflow
- Adding Controller Configuration Groups
- Configuring Controller Configuration Groups
- Adding or Removing Controllers from a Configuration Group
- Adding or Removing Templates from the Configuration Group
- Auditing Configuration Groups
- Rebooting Configuration Groups

---

**Auditing Configuration Groups**

The Configuration Groups Audit page allows you to verify if the configuration of the controller complies with the group templates and mobility group.

When auditing the Configuration Groups:

1. You can leave this screen or log out of Prime Infrastructure. The process continues, and you can return to this page later to view a report.

2. Do not perform any other configuration group functions during the audit verification.

3. This audit does not enforce the Prime Infrastructure configuration to the device. It only identifies the discrepancies.

To perform a configuration group audit, follow these steps:

**Step 1** Choose **Configuration > Templates > Controller Configuration Groups**, and click a group name in the Group Name column.

**Step 2** Click the **Audit** tab to access this page.

**Step 3** Click to highlight a controller from the **Controllers** tab, choose **>> (Add)**, and **Save Selection**.

**Step 4** Click to highlight a template from the **Templates** tab, choose **>> (Add)**, and **Save Selection**.

**Step 5** Click **Audit** to begin the auditing process.

A report is generated and the current configuration on each controller is compared with that in the configuration group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.
Rebooting Configuration Groups

Step 6 Click **Details** to view the Controller Audit Report details.

Step 7 Double-click a line item to open the Attribute Differences page. This page displays the attribute, its value in Prime Infrastructure, and its value in the controller.

Step 8 Click **Retain Prime Infrastructure Value** to push all attributes in the Attribute Differences page to the device.

Step 9 Click **Close** to return to the Controller Audit Report page.

---

**Rebooting Configuration Groups**

To reboot a configuration group, follow these steps:

Step 1 Choose **Configuration > Templates > Controller Configuration Groups**, and click a group name in the Group Name column.

Step 2 Click the **Reboot** tab.

Step 3 Check the **Cascade Reboot** check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.

Step 4 Click **Reboot** to reboot all controllers in the configuration group at the same time. During the reboot, you can leave this page or logout of Prime Infrastructure. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report page shows when each controller was rebooted and what the controller status is after the reboot. If Prime Infrastructure is unable to reboot the controller, a failure is shown.

If you want to print the report as shown on the page, you must choose landscape page orientation.

---

**Related topics**

- Configuring Controller Mobility Groups: Workflow
- Adding Controller Configuration Groups
- Configuring Controller Configuration Groups
- Adding or Removing Controllers from a Configuration Group
- Adding or Removing Templates from the Configuration Group
- Applying or Scheduling Configuration Groups
- Rebooting Configuration Groups
Viewing Configuration Group Reports

To display all recently applied reports under a specified group name, follow these steps:

**Step 1** Choose Configuration > Templates > Controller Configuration Groups, and click a group name in the Group Name column.

**Step 2** Click the Report tab. The Recent Apply Report page displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:

- **Apply Status**—Indicates success, partial success, failure, or not initiated.
- **Successful Templates**—Indicates the number of successful templates associated with the applicable IP address.
- **Failures**—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
- **Details**—Click Details to view the individual failures and associated error messages.

**Step 3** If you want to view the scheduled task reports, click the click here link at the bottom of the page. You are then redirected to the Configure > Scheduled Configuration Tasks > Configuration Group menu where you can view reports of the scheduled configuration groups.

**Related Topics**
- Adding Controller Configuration Groups
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups

**Downloading Software to Configuration Groups**

To download software to all controllers in the selected groups after you have established a configuration group, follow these steps:

**Step 1** Choose Configuration > Templates > Controller Configuration Groups.

**Step 2** Select the check box to choose one or more configuration groups names on the Configuration Groups page.

**Step 3** Choose Download Software from the Select a command drop-down list, and click Go.

**Step 4** The Download Software to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose local machine from the File is Located On field.

**Step 5** Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.

**Step 6** Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.
Step 7  The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click Browse to navigate to it. The controller uses this local filename as a base name and then adds _custom.sgi as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.

Step 8  Click OK.

Related topics
- Downloading IDS Signatures to Configuration Groups
- Downloading Customized WebAuth to Configuration Groups

---

**Downloading IDS Signatures to Configuration Groups**

To download Intrusion Detection System (IDS) signature files from your configuration group to a local TFTP server, follow these steps:

---

Step 1  Choose Configuration > Templates > Controller Configuration Groups.
Step 2  Select the check box to choose one or more configuration groups on the Configuration Groups page.
Step 3  Choose Download IDS Signatures from the Select a command drop-down list, and click Go.
Step 4  The Download IDS Signatures to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed. Choose local machine from the File is Located On field.
Step 5  Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries field.
Step 6  Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout field.
Step 7  The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click Browse to navigate to it. The controller uses this local filename as a base name and then adds _custom.sgi as a suffix.

If the transfer times out for some reason, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried.

Step 8  Click OK.

Related topics
- Downloading Software to Configuration Groups
- Downloading Customized WebAuth to Configuration Groups

---

**Downloading Customized WebAuth to Configuration Groups**

To download customized web authentication, follow these steps:
Step 1: Choose Configuration > Templates > Controller Configuration Groups.

Step 2: Select the check box to choose one or more configuration groups on the Configuration Groups page.

Step 3: Choose Download Customized WebAuth from the Select a command drop-down list, and click Go.

Step 4: The Download Customized Web Auth Bundle to Controller page appears. The IP address of the controller to receive the bundle and the current status are displayed.

Step 5: Choose local machine from the File is Located On field.

Related topics
- Downloading Software to Configuration Groups
- Downloading IDS Signatures to Configuration Groups

About Mobility

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another, securely and with as little latency as possible, in a wireless network. When a wireless client is associated to and authenticated by an access point, a controller places an entry for that client in its client database. This entry includes the MAC and IP addresses of the client, security context and associations, quality of service (QoS) contexts, the WLANs, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client.

Related Topics
- Intra-Controller Roaming
- Inter-Controller Roaming
- Inter-Subnet Roaming
- Working with Wireless Mobility

Intra-Controller Roaming

When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well. Figure 28-1 illustrates a wireless client roaming from one access point to another when both access points are connected to the same controller.
About Mobility

Figure 28-1  Intra-Controller Roaming

Inter-Controller Roaming

When a client roams from an access point connected to one controller to an access point connected to a different controller, the process also varies based on whether the controllers are operating on the same subnet. Figure 28-2 illustrates inter-controller roaming, which occurs when the wireless LAN interfaces of a controller are on the same IP subnet.

When the client is associated to an access point connected to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains invisible to the user.

All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication to comply with the IEEE standard.
Inter-Subnet Roaming

Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on how the client roams. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains invisible to the wireless client, and the client maintains its original IP address.

After an inter-subnet roam, data flows in an asymmetric traffic path to and from the wireless client. Traffic from the client to the network is forwarded directly into the network by the foreign controller. Traffic to the client arrives at the anchor controller, which forwards the traffic to the foreign controller in an EtherIP tunnel. The foreign controller then forwards the data to the client. If a wireless client roams to a new foreign controller, the client database entry is moved from the original foreign controller to the new foreign controller, but the original anchor controller is always maintained. If the client moves back to the original controller, it becomes local again.
In inter-subnet roaming, WLANs on both anchor and foreign controllers need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients might have network connectivity problems after the handoff.

Inter-subnet roaming does not support multicast traffic such as one used by Spectralink phones while using push-to-talk. **Figure 28-3** illustrates *inter-subnet roaming*, which occurs when the wireless LAN interfaces of a controller are on different IP subnets.

**Figure 28-3  Inter-Subnet Roaming**

![Inter-Subnet Roaming Diagram](image)

Related topics
- About Mobility
- About Mobility Groups
- Intra-Controller Roaming
- Inter-Controller Roaming
- When to Include Controllers in a Mobility Group

**Symmetric Tunneling**

With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Filtering (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled. All controllers in a mobility group should have the same symmetric tunneling mode.
About Mobility Groups

With this feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

A set of controllers can be configured as a mobility group to allow seamless client roaming within a group of controllers. This enables multiple controllers to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of clients and controller loading information. With this information, the network can support inter-controller wireless LAN roaming and controller redundancy. Clients do not roam across mobility groups.

Figure 28-4 shows an example of a mobility group.

As shown in Figure 28-4, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. All mobility exchange traffic between controllers is carried over a CAPWAP tunnel.

Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group consisting of 24 4404-100 controllers supports up to 2400 access points (24 * 100 = 2400 access points).
2. A 4402-25 controller supports up to 25 access points, and a 4402-50 controller supports up to 50 access points. Therefore, a mobility group consisting of 12 4402-25 controllers and 12 4402-50 controllers supports up to 900 access points (12 * 25 + 12 * 50 = 300 + 600 = 900 access points).

Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless network. Figure 28-5 shows the results of creating distinct mobility group names for two groups of controllers.

**Figure 28-5 Two Mobility Groups**

The controllers in the ABC mobility group recognize and communicate with each other through their access points and through their shared subnets. The controllers in the ABC mobility group do not recognize or communicate with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not recognize or communicate with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network. Clients might roam between access points in different mobility groups, provided they can detect them. However, their session information is not carried between controllers in different mobility groups.

**Related Topics**
- When to Include Controllers in a Mobility Group
- Messaging Among Mobility Groups

**When to Include Controllers in a Mobility Group**

If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.
Messaging Among Mobility Groups

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. In Prime Infrastructure and controller software releases 5.0, two improvements have been made to mobility messaging, each of which is especially useful when sending messages to the full list of mobility members:

- Sending Mobile Announce messages within the same group first and then to other groups in the list
  The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it. In the software releases prior to 5.0, the controller sends this message to all members in the list irrespective of the group to which they belong. However, in the software release 5.0, the controller sends the message only to those members that are in the same group as the controller and then includes all of the other members while sending retries.

- Sending Mobile Announce messages using multicast instead of unicast
  In Prime Infrastructure and controller software releases prior to 5.0, the controller might be configured to use multicast to send the mobile announce messages, which requires sending a copy of the messages to every mobility member. This behavior is not efficient because many messages (such as Mobile Announce, Pairwise Master Key (PMK) Update, AP List Update, and Intrusion Detection System (IDS) Shun) are meant for all members in the group. In Prime Infrastructure and controller software releases 5.0, the controller uses multicast mode to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group containing all the mobility members. To derive the maximum benefit from multicast messaging, we recommend that it be enabled or disabled on all group members.

Related Topics

- About Mobility Groups
- When to Include Controllers in a Mobility Group
- Configuring Mobility Groups: Workflow

Configuring Mobility Groups: Workflow

Whenever you configure a Mobility Group, follow this workflow:

1. Make sure you have gathered the information you need and that the participating controller are properly configured, as explained in “Before You Begin Configuring Mobility Groups”.

2. Add individual controllers to the Mobility Group. You may need to add them manually if no Mobility Groups exist or no controllers are listed when you try to add them from the Configuration> Network > Network Devices page.

3. Set the scale and messaging parameters for the Mobility Group.
Before You Begin Configuring Mobility Groups

Before you add controllers to a mobility group, you must verify that the following requirements have been met for all controllers that are to be included in the group:

- All controllers must be configured for the same LWAPP transport mode (Layer 2 or Layer 3). Verify and change the LWAPP transport mode by navigating to Administration > Settings > System Settings > General page.
- Verify IP connectivity by pinging the controllers and make sure IP connectivity exists between the management interfaces of all devices.
- All controllers must be configured with the same mobility group name for seamless routing among the access points.
- All devices must be configured with the same virtual interface IP address, else client loses connectivity for a period of time, though inter-controller roaming appears to be working.
- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you configure all controllers with the MAC address and IP address of all the other mobility group members.

Adding Controllers to Mobility Groups

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name for a controller. This allows you to access the controller templates interface for the controller you are managing.

Step 3 Choose System > Mobility Groups from the left sidebar menu. The existing Mobility Group members are listed in the page.

Step 4 You see a list of available controllers. From the Select a command drop-down list in the upper right-hand corner, choose Add Group Members and then click Go.

Step 5 Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The group address of the local mobility member must be the same as the group address of the local controller.

Step 6 In the Group Name text box, enter the name of the mobility group.
Step 7  Click Save.

Step 8  Repeat steps 1 through 8 for the remaining controllers.

Related Topics

- Configuring Mobility Groups: Workflow
- Before You Begin Configuring Mobility Groups
- Adding Controllers to Mobility Groups Manually
- Setting Mobility Scalability Parameters

Adding Controllers to Mobility Groups Manually

You can add controllers to Mobility Groups manually if you cannot display a list of existing Mobility Groups and available controller.

Step 1  Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2  Click on a Device Name for a controller. This allows you to access the controller templates interface for the controller you are managing.

Step 3  The Wireless Controller page appears. Click Configuration tab.

Step 4  Choose System > Mobility Groups from the left sidebar menu. The existing Mobility Group members are listed in the page.

Step 5  You see a list of available controllers. From the Select a command drop-down list in the upper right-hand corner, choose Add Group Members and then click Go.

Step 6  If you don't see a list of controllers, click the “To add members manually to the Mobility Group click here” link. The Mobility Group Member page appears.

Step 7  In the Member MAC Address text box, enter the MAC address of the controller to be added.

Step 8  In the Member IP Address text box, enter the management interface IP address of the controller to be added.

If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the management interface IP address of the controller. Otherwise, mobility fails among controllers in the mobility group.

Step 9  Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The group address of the local mobility member must be the same as the group address of the local controller.

Step 10 In the Group Name text box, enter the name of the mobility group.

Step 11 Click Save.

Step 12 Repeat steps 1 through 12 for the remaining controllers.

Related Topics

- Configuring Mobility Groups: Workflow
Setting Mobility Scalability Parameters

Complete the procedure of Adding Controllers To Mobility Groups before setting the mobility message parameters.

**Step 1** Choose **Configuration > Network > Network Devices**, then from the Device Groups menu on the left, select **Device Type > Wireless Controller**.

**Step 2** Click on a Device Name for a controller whose software version is 5.0 or later.

**Step 3** The Wireless Controller page appears. Click **Configuration** tab.

**Step 4** Choose **System > Multicast** from the left sidebar menu. The Multicast page appears.

**Step 5** Choose **Multicast** or **Unicast** from the **Ethernet Multicast Support** drop-down list.

**Step 6** Enter the group IP address at the Multicast Group Address field, if you chose multicast in Step 4, to begin multicast mobility messaging. You must also configure this IP address for the local mobility group, but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

**Step 7** Select the **Global Multicast Mode** check box to make the multicast mode available globally.

**Step 8** Choose **Enable** from the **Multicast Mobility Mode** drop-down list, and enter the mobility group multicast address.

**Step 9** Select the **Multicast Direct** check box to enable videos to be streamed over a wireless network.

**Step 10** Specify the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream. All media streams on a controller share this configuration.

   a. **State**—Select the check box to activate the Session Banner. If not activated, the Session Banner is not sent to the client

   b. **URL**—A web address reported to the client

   c. **Email**—An e-mail address reported to the client

   d. **Phone**—A telephone number reported to the client

   e. **Note**—A note reported to the client

**Step 11** Click **Save**.

**Related Topics**

- Configuring Mobility Groups: Workflow
- Before You Begin Configuring Mobility Groups
- Adding Controllers to Mobility Groups
- Adding Controllers to Mobility Groups Manually
Mobility Anchors

Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN. This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of a client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographic load balancing because WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on).

Related Topic
- Mobility Anchors
- Configuring Multiple Country Codes
- Adding Multiple Controllers And Setting DCA Channels

Adding Multiple Controllers And Setting DCA Channels

Step 1 Choose Configuration > Templates > Controller Configuration Groups.
Step 2 Choose Add Configuration Groups from the Select a command drop-down list, and click Go.
Step 3 Create a configuration group by entering the group name and mobility group name.
Step 4 Click Save. The Configuration Groups page appears.
Step 5 Click the Controllers tab. The Controllers page appears.
Step 6 Highlight the controllers you want to add, and click Add. The controller is added to the Group Controllers page.
Step 7 Click the Country/DCA tab. The Country/DCA page appears. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.
Step 8 Check the Update Country/DCA check box to display a list of countries from which to choose.
Step 9 Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes page. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking Save Selection.

Configuring Controller Mobility Groups: Workflow

By creating a configuration group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all the controllers in a group. You can add, delete, or remove configuration groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected configuration groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected configuration groups.
Before You Begin

- Bear in mind that a controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

- By choosing Configuration > Templates > Controller Configuration Groups, you can view a summary of all configuration groups in the Prime Infrastructure database. When you choose Add Configuration Groups from the Select a command drop-down list, the page displays a table with the following columns:
  - Group Name: Name of the configuration group.
  - Templates: Number of templates applied to configuration group.

Related topics

- Adding Controller Configuration Groups
- Configuring Controller Configuration Groups
- Adding or Removing Controllers from a Configuration Group
- Adding or Removing Templates from the Configuration Group
- Applying or Scheduling Configuration Groups
- Auditing Configuration Groups
- Rebooting Configuration Groups
Chokepoints

Chokepoints are low frequency transmitting devices. When a tag passes within range of placed chokepoint, the low-frequency field awakens the tag that in turn sends a message over the Cisco Unified Wireless Network including the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room level accuracy (ranging from few inches to 2 feet depending on the vendor).

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on a the Prime Infrastructure map.

Related Topics

- Adding Chokepoints
- Editing Chokepoints

Adding Chokepoints

To add a chokepoint, follow these steps:

**Step 1** Choose **Configuration > Wireless Technologies > Chokepoints**.

**Step 2** From the Select a command drop-down list, choose **Add Chokepoints**, then click **Go**.

**Step 3** Enter the MAC address and name for the chokepoint.

**Step 4** Select the check box to indicate that it is an Entry/Exit Chokepoint.

**Step 5** Enter the coverage range for the chokepoint.
Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

**Step 6**
Click OK.

After the chokepoint is added to the database, it can be placed on the appropriate the Prime Infrastructure floor map.

---

**Removing Chokepoints**

To remove a chokepoint, follow these steps:

**Step 1** Choose **Configuration > Wireless Technologies > Chokepoints**.

**Step 2** Select the check box of the chokepoint that you want to delete.

**Step 3** From the Select a command drop-down list, choose **Remove Chokepoints**, then click **Go**.

**Step 4** Click **OK** to confirm the deletion.

---

**Related Topics**
- Editing Chokepoints

**Adding Chokepoints to Maps**

To add a chokepoint to a map, follow these steps:

**Step 1** Choose **Maps > Wireless Maps > Site Maps**.

**Step 2** Click the link that corresponds to the floor location of the chokepoint.

**Step 3** From the Select a command drop-down list, choose **Add Chokepoints**.

**Step 4** Click **Go**.

The Add Chokepoints summary page lists all recently-added chokepoints that are in the database but not yet mapped.

**Step 5** Select the check box next to the chokepoint that you want to place on the map.

**Step 6** Click **OK**.

A map appears with a chokepoint icon located in the top-left hand corner. You are now ready to place the chokepoint on the map.

**Step 7** Left-click the chokepoint icon and drag and place it in the proper location. The MAC address, name, and coverage range of the chokepoint appear in the selected chokepoints detail page when you click the chokepoint icon for placement.

**Step 8** Click **Save**.

You are returned to the floor map and the added chokepoint appears on the map.

The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.
The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint display when you pass a mouse over its map icon.

**Step 9**
If the chokepoint does not appear on the map, select the **Chokepoints** check box located in the Floor Settings menu.

Do not select the **Save Settings** check box unless you want to save this display criteria for all maps.

**Step 10**
You must synchronize network design to the mobility services engine or location server to push chokepoint information.

---

**Removing Chokepoints from Maps**

To remove an chokepoint from the map, follow these steps:

**Step 1**
Choose **Maps > Wireless Maps > Site Maps**.

**Step 2**
In the Maps page, choose the link that corresponds to the floor location of the chokepoint.

**Step 3**
From the Select a command drop-down list, choose **Remove Chokepoints**.

**Step 4**
Click **Go**.

**Step 5**
Click **OK** to confirm the deletion.

---

**Editing Chokepoints**

To edit a current chokepoint, follow these steps:

**Step 1**
Choose **Configuration > Wireless Technologies > Chokepoints**. The following information is displayed for each current chokepoint: MAC address, chokepoint name, entry/exit chokepoint, range, static IP address, and map location for the chokepoint.

**Step 2**
Click the chokepoint you want to edit in the MAC Address column.

**Step 3**
Edit the following parameters, as necessary:
- Name
- Entry/Exit Chokepoint—Click to enable.
- Range—Coverage range for the chokepoint.

The chokepoint range is product-specific and is supplied by the chokepoint vendor.

- Static IP Address

**Step 4**
Click **Save**.
Wi-Fi TDOA Receivers

- Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting, page 29-iv
- Adding Wi-Fi TDOA Receivers, page 29-iv
- Editing Wi-Fi TDOA Receivers, page 29-vi

Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset. TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

- If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.
- The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network. See Adding MSEs to Prime Infrastructure for details on adding a mobility services engine.
2. Add the TDOA receiver to the Prime Infrastructure database and map. See Adding Wi-Fi TDOA Receivers for details on adding the TDOA receiver to the Prime Infrastructure.
3. Activate or start the partner engine service on the MSE using the Prime Infrastructure.
4. Synchronize the Prime Infrastructure and mobility services engines. See Synchronizing Prime Infrastructure and a Mobility Services Engine for details on synchronization.
5. Set up the TDOA receiver using the AeroScout System Manager.

See the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User’s Guide for configuration details at the following URL:

Related Topics
- Adding Wi-Fi TDOA Receivers
- Editing Wi-Fi TDOA Receivers
- Editing Wi-Fi TDOA Receivers

Adding Wi-Fi TDOA Receivers

After the Wi-Fi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on an Prime Infrastructure map.
After adding TDOA receivers to the Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than the Prime Infrastructure.

For more details on configuration options, see the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide at the following URL: http://support.aeroscout.com.

To add a TDOA receiver to the Prime Infrastructure database and appropriate map, follow these steps:

**Step 1** Choose **Configuration > Wireless Technologies > WiFi TDOA Receivers** to open the All WiFi TDOA Receivers summary page.

To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

**Step 2** From the Select a command drop-down list, choose **Add WiFi TDOA Receivers**, then click **Go**.

**Step 3** Enter the MAC address, name and static IP address of the TDOA receiver.

**Step 4** Click **OK** to save the TDOA receiver entry to the database.

After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate Prime Infrastructure floor map.

A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

### Related Topic
- Editing Wi-Fi TDOA Receivers

### Adding Wi-Fi TDOA Receivers to Maps

**Step 1** To add the TDOA receiver to a map, choose **Maps > Wireless Maps > Site Maps**.

**Step 2** In the Maps page, select the link that corresponds to the floor location of the TDOA receiver.

**Step 3** From the Select a command drop-down list, choose **Add WiFi TDOA receivers**, then click **Go**.

**Step 4** Select the check box next to each TDOA receiver to add it to the map.

**Step 5** Click **OK**. A map appears with a TDOA receiver icon located in the top-left hand corner. You are now ready to place the TDOA receiver on the map.

**Step 6** Left-click the TDOA receiver icon and drag and place it in the proper location on the floor map.

The MAC address and name of the TDOA receiver appear in the left pane when you click the TDOA receiver icon for placement.

**Step 7** Click **Save** when the icon is placed correctly on the map. The added TDOA receiver appears on the floor heat map.

The icon for the newly added TDOA receiver might or might not appear on the map depending on the display settings for that floor.

**Step 8** If the TDOA receiver does not appear on the map, click **Layers** to collapse a selection menu of possible elements to display on the map.

**Step 9** Select the **WiFi TDOA Receivers** check box. The TDOA receiver appears on the map.

When you place your cursor over a TDOA receiver on a map, configuration details display for that receiver.
Step 10  Click X to close the Layers page.  
Do not choose Save Settings from the Layers menu unless you want to save this display criteria for all maps.

Step 11  You can now download the partner engine software to the mobility services engine.

Related Topics
- Using Wi-Fi TDOA Receivers to Enhance Tag Location Reporting
- Editing Wi-Fi TDOA Receivers

Editing Wi-Fi TDOA Receivers

To view a current TDOA receiver to the Prime Infrastructure database, follow these steps:

Step 1  Choose Configuration > Wireless Technologies > WiFi TDOA Receivers to open the All WiFi TDOA Receivers summary page.

Step 2  Click the MAC Address link to view the TDOA receiver details including MAC address, name, and static IP address.

Step 3  Make the necessary changes to the receiver name or IP address, then click Save to confirm these changes.  
A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Removing Wi-Fi TDOA Receivers

You can remove one or multiple WiFi TDOA receivers at a time. If you remove a TDOA receiver from a map it remains in the Prime Infrastructure database but is labeled as unassigned.

To delete a TDOA receiver from the Prime Infrastructure, follow these steps:

Step 1  Choose Configuration > Wireless Technologies > WiFi TDOA Receivers.  
Step 2  Select the check box next to each TDOA receiver to be deleted.
Step 3  From the Select a command drop-down list, choose Remove WiFi TDOA Receivers, then click Go.  
Step 4  To confirm TDOA receiver deletion, click OK in the dialog box.  
In the All WiFi TDOA Receivers page, a message confirms the deletion. The deleted TDOA receiver is no longer listed in the page.

Access Point Radios

- Adding Autonomous Access Points to Prime Infrastructure
Adding Autonomous Access Points to Prime Infrastructure

From Prime Infrastructure, the following methods are available for adding autonomous access points:

- Removing Autonomous Access Points, page 29-x

Adding Autonomous Access Points by Device Information

Autonomous access points can be added to Prime Infrastructure by device information using comma-separated IP addresses and credentials.

Cisco autonomous access points are shipped from the factory with Cisco as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the console port of an access point.

To add autonomous access points using device information, follow these steps:

**Step 1** Choose Configuration > Wireless Technologies > Access Point Radios.

**Step 2** From the Select a command drop-down list, choose Add Autonomous APs, click Go.

**Step 3** Choose Device Info from the Add Format Type drop-down list.

**Step 4** Enter comma-separated IP addresses of autonomous access points.

**Step 5** Enter the SNMP Parameters parameters:
- Version—Choose from v1, v2, or v3.
- Retries—Indicates the number of controller discovery attempts.
- Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The valid range is 2 to 90 seconds. The default is 10 seconds.
- Community—Public or Private.

**Step 6** Enter the Telnet/SSH Parameters:
Default values are used if the Telnet/SSH parameters are left blank.
- Protocol—Select the protocol you want to use (either Telnet or SSH).
- User Name—Enter the username. (The default username is admin.) The Telnet/SSH username must have sufficient privileges to execute commands in CLI templates.
- Password/Confirm Password—Enter and confirm the password. (Default password is admin.)
- Enable Password/Confirm Password—Enter and confirm an enable password.
- Telnet Timeout—Indicate the amount of time (in seconds) allowed before the process time outs. The default is 60 seconds.

**Step 7** Click Add.

After the AP is added and its inventory collection is completed, it appears in the Access Point list page (Configure > Access Points). If it is not found in the Access Points list, choose Configure > Unknown Device page to check the status.
Autonomous access points are not counted towards the total device count for your license.

## Adding Autonomous Access Points by CSV File

Autonomous access points can be added to Prime Infrastructure using a CSV file exported from WLSE. To add autonomous access points using a CSV file, follow these steps:

1. Choose **Configuration > Wireless Technologies > Access Point Radios**.
2. From the Select a command drop-down list, choose **Add Autonomous APs**, click **Go**.
3. Choose **File** from the Add Format Type drop-down list.
4. Enter or browse to the applicable CSV file.

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries, snmp_timeout, telnet_username, telnet_password, telnet_retries, telnet_timeout
209.165.200.224, 255.255.255.224, v2, public, , , , , , 3, 4
209.165.201.0, 255.255.255.0, v2, public, , , , , , 3, 4, Cisco, Cisco, 2, 10
```

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries, snmp_timeout, telnet_username, telnet_password, telnet_retries, telnet_timeout
209.165.200.224, 255.255.255.224, v3, default, HMAC-MD5, default, None, None, 3, 4
209.165.201.0, 255.255.255.224, v3, default1, HMAC-MD5, default1, DES, default1, 3, 4, Cisco, Cisco, 2, 10
```

The CSV files can contain the following fields:

- `ip_address`
- `network_mask`
- `snmp_version`
- `snmp_community`
- `snmpv3_user_name`
- `snmpv3_auth_type`
- `snmpv3_auth_password`
- `snmpv3_privacy_type`
- `snmpv3_privacy_password`
- `snmp_retries`
- `snmp_timeout`
- `telnet_username`
Bulk Update of Autonomous Access Points

You can update multiple autonomous access points credentials by importing a CSV file.

To update autonomous access point(s) information in a bulk, follow these steps:

**Step 1** Choose Configuration > Wireless Technologies > Access Point Radios.

**Step 2** Select the check box(es) of the applicable controller(s).

**Step 3** From the Select a command drop-down list, choose Bulk Update APs. The Bulk Update Autonomous Access Points page appears.

**Step 4** Click Choose File to select a CSV file, and then find the location of the CSV file you want to import.

**Step 5** Click Update and Sync.

**Related Topics**
- Sample CSV File for the Bulk Update of Autonomous Access Points

**Sample CSV File for the Bulk Update of Autonomous Access Points**

The sample CSV files for V2 devices are as follows:

```
209.165.200.224,255.255.255.224,v2,public,,,,3,4
209.165.201.0,255.255.255.0,v2,public,,,,,,,,,3,4,Cisco,Cisco,2,10
```

**Note** The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4
209.165.201.0,255.255.255.0,v3,default1,HMAC-MD5,default1,DES,DES,3,10
```

The CSV files can contain the following fields:
- ip_address
- network_mask
Removing Autonomous Access Points

**Note**
If you replace Autonomous Access Points because of some reason, remove the Autonomous Access Points from Prime Infrastructure before you install the replacement access points on the network.

To remove an autonomous access point from Prime Infrastructure, follow these steps:

**Step 1** Select the check boxes of the access points you want to remove. Select the APs that are not associated.

**Step 2** Choose Remove APs from the Select a command drop-down list.

Viewing Autonomous Access Points in Prime Infrastructure

Once added, the autonomous access points can be viewed on the Monitor > Access Points page.

Click the autonomous access point to view more detailed information such as the following:

- Operational status of the access points
- Key attributes including radio information, channel, power, and number of clients on the radio
- CDP neighbored information

The autonomous access points can also be viewed in Monitor > Maps. They can be added to a floor area by choosing Monitor Maps > floor area and choosing Add Access Points from the Select a command drop-down list.
**Downloading Images to Autonomous Access Points (TFTP)**

Lightweight access point images are bundled with controller images and managed by the controller. Autonomous access point images must be handled by a NMS system such as WLSE, CiscoWorks, or Prime Infrastructure.

To download images to autonomous access points using TFTP, follow these steps:

**Step 1** Choose **Configuration > Wireless Technologies > Access Point Radios**.

**Step 2** Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

**Step 3** From the Select a command drop-down list, choose **Download Autonomous AP Image (TFTP)**. The Download images to Autonomous APs page appears.

**Step 4** Configure the following parameters:

- File is located on—Choose **Local machine** or **TFTP server**.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the TFTP server IP address. This is automatically populated if the default server is selected.
- Prime Infrastructure Server Files In—Specify where Prime Infrastructure server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the server filename.

**Step 5** Click **Download**.

*Tip* Some TFTP servers might not support files larger than 32 MB.

---

**Downloading Images to Autonomous Access Points (FTP)**

To download images to autonomous access points (using FTP), follow these steps:

**Step 1** Choose **Configuration > Wireless Technologies > Access Point Radios**

**Step 2** Select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

**Step 3** From the Select a command drop-down list, choose **Download Autonomous AP Image (FTP)**. The Download images to Autonomous APs page appears.

**Step 4** Enter the FTP credentials including username and password.

**Step 5** Configure the following parameters:

- File is located on—Choose **Local machine** or **FTP server**.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the FTP server IP address. This is automatically populated if the default server is selected.
Supporting Autonomous Access Points in Work Group Bridge (WGB) mode

Workgroup Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The WGB and its wired clients are listed as clients in Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all Prime Infrastructure clients that are WGBs, choose **Monitor > Clients**. From the Show drop-down list, choose **WGB Clients**, and click **Go**. The Clients (detected as WGBs) page appears. Click a user to view detailed information regarding a specific WGB and its wired clients.

Note
Prime Infrastructure provides WGB client information for the autonomous access point whether or not it is managed by Prime Infrastructure. If the WGB access point is also managed by Prime Infrastructure, Prime Infrastructure provides basic monitoring functions for the access point similar to other autonomous access points.

Configuring Access Point Details

Choose **Configuration > Wireless Technologies > Access Point Radios** to see a summary of all access points in Prime Infrastructure database. The summary information includes the following:

- Ethernet MAC
- IP Address
- Radio
- Map Location
- AP Type
- Controller
- Operation Status
- Alarm Status
- Audit Status

Note If you hover your mouse cursor over the Audit Status value, the time of the last audit is displayed.

Note You can click the **Edit View** link to add, remove or reorder columns such as AP Mode, Channel Width, Client Count, and so on.
Step 1  Click the link in the AP Name column to see detailed information about that access point name. The Access Point Detail page appears.

Note  The operating system software automatically detects and adds an access point to Prime Infrastructure database as it associates with existing controllers in Prime Infrastructure database.

Note  Access point parameters might vary depending on the access point type.

Some of the parameters on the page are automatically populated.

- The General group box displays the AP Name, Ethernet MAC, Base Radio MAC, IP Address, Admin Status, AP Static IPv4/IPv6, AP Mode, AP Sub Mode, AP Failover Priority, Registered Controller, Primary Controller Name, Secondary Controller Name, Tertiary Controller Name, Primary Controller Management IP, Secondary Controller Management IP, Tertiary Controller Management IP, AP Group Name, Location, Statistics Timer.

- The Versions group box of the page displays the software and boot version.

- The Inventory Information group box displays the model, AP type, AP certificate type, serial number, and REAP mode support, FlexConnect mode support.

- The Ethernet Interfaces group box provides information such as interface name, slot ID, admin status, and CDP state.

- The Radio Interfaces group box provides the current status of 802.11a/n, 802.11ac, 802.11b/g/n, and XOR (2.4 GHz), XOR (5GHz), or XOR (Monitor Mode) radios with the information such as admin status, channel number, power level, antenna mode, antenna diversity, and antenna type.

To set the configurable parameters, follow these steps:

Note  Changing access point parameters causes the access point to be temporarily disabled and this might cause some clients to lose connectivity.

Step 2  Enter the name assigned to the access point.

Step 3  Use the drop-down list to choose a country code to establish multiple country support. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that the access point complies with the regulations of your country. Consider the following when setting the country code:

- You can configure up to 20 countries per controller.

- Because only one auto-RF engine and one list of available channels exist, configuring multiple countries limits the channels available to auto-RF in the common channels. A common channel is one that is legal in each and every configured country.

- When you configure access points for multiple countries, the auto-RF channels are limited to the highest power level available in every configured country. A particular access point might be set to exceed these limitations (or you might manually set the levels in excess of these limitations), but auto-RF does not automatically choose a non-common channel or raise the power level beyond that available in all countries.
Note

Access points might not operate properly if they are not designed for use in your country of operation. For example, an (-A) access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Europe (-E). Always be sure to purchase access points that match the regulatory domain of your country. For a complete list of country codes supported per product, see this URL:


Step 4 If you want to enable the access point for administrative purposes, select the Enable check box.

Step 5 If you click Enable at the AP Static IP check box, a static IP address is always assigned to the access point rather than getting an IP address dynamically upon reboot.

Step 6 Choose the role of the access point from the AP Mode drop-down list. No reboot is required after the mode is changed except when monitor mode is selected. You are notified of the reboot when you click Save. The available modes are as follows:

- Local—This is the normal operation of the access point and the default AP Mode choice. With this mode, data clients are serviced while configured channels are scanned for noise and rogues. The access point goes off-channel for 50 ms and listens for rogues. It cycles through each channel for the period specified under the Auto RF configuration.

  AP Sub Mode—When the AP Mode is set to Local, you can set the AP Sub Mode to WIPS.

- FlexConnect—Choose FlexConnect from the AP Mode drop-down list to enable FlexConnect for up to six access points. The FlexConnect access points can switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

  Note To configure Local or FlexConnect access points for Cisco Adaptive wIPS feature, choose Local or FlexConnect, and select the Enhanced wIPS Engine Enabled check box.

  AP Sub Mode - When the AP Mode is set to FlexConnect, you can set the AP Sub Mode to any one of the following:

  - WIPS
  - PPPOE—To configure the Point-to-Point Protocol over Ethernet (PPPoE) submode on the access point.
  - PPPOE-WIPS—To configure both Point Protocol over Ethernet (PPPoE) and wIPS submodes on the access point.

- Monitor—This is radio receive only mode and allows the access point to scan all configured channels every 12 seconds. Only deauthentication packets are sent in the air with an access point configured this way. A monitor mode access point detects rogues, but it cannot connect to a suspicious rogue as a client to prepare for the sending of RLDP packets.

  AP Sub Mode—When the AP Mode is set to Monitor, you can set the AP Sub Mode to WIPS.
Access Point Radios

Note You can expand the monitor mode for tags to include location calculation by enabling the tracking optimized monitor mode (TOMM) feature. When TOMM is enabled, you can specify which four channels within the 2.4 GHz band (802.11b/g radio) of an access point to use to monitor tags. This allows you to focus channel scans on only those channels for which tags are traditionally found (such as channels 1, 6, and 11) in your network. To enable TOMM, you must also make additional edits on the 802.11b/g radio of the access point. See the “Configuring Access Point Radios for Tracking Optimized Monitor Mode” section on page 29-xxxv for configuration details.

Note You cannot enable both TOMM and wIPS at the same time. TOMM can be enabled only when wIPS is disabled.

Note To configure access points for Cisco Adaptive wIPS feature, choose Monitor and select the Enhanced wIPS Engine Enabled check box, and select wIPS from the Monitor Mode Optimization drop-down list.

- Rogue Detector—In this mode, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.

- Sniffer—Operating in sniffer mode, the access point captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. These packets contain information such as timestamp, signal strength, packet size, and so on. This feature can only be enabled if you run AiroPeek, which is a third-party network analyzer software that supports the decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com.

- Bridge—Bridge mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The bridge and its wired clients are listed as client in Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.

- SE-Connect—This mode allows a CleanAir-enabled access point to be used extensively for interference detection on all monitored channels. All other functions such as IDS scanning and Wi-Fi are suspended.

Note This option is displayed only if the access point is CleanAir-capable.

Note Changing the AP mode reboots the access point.

Step 7 Disable any access point radios.

Step 8 From the AP Failover Priority drop-down list, choose Low, Medium, High, or Critical to indicate the failover priority of the access point. The default priority is low.
**Step 9** In the Primary, Secondary, and Tertiary Controller fields, you can define the order in which controllers are accessed.

**Step 10** The AP Group Name drop-down shows all access point group names that have been defined using WLANs > AP Group VLANs, and you can specify whether this access point is tied to any group.

**Note** An access point group name to 31 characters for WLC versions earlier than 4.2.132.0 and 5.0.159.0.

**Step 11** Enter a description of the physical location where the access point was placed.

**Step 12** In the Stats Collection Period field, enter the time in which the access point sends .11 statistics to the controller. The valid range is 0 to 65535 seconds. A value of 0 means statistics should not be sent.

**Step 13** Choose **Enable** for Mirror Mode if you want to duplicate (to another port) all of the traffic originating from or terminating at a single client device or access point. Mirror mode is useful in diagnosing specific network problems but should only be enabled on an unused port since any connections to this port become unresponsive.

**Step 14** You can globally configure MFP on a controller. When you do, management frame protection and validation are enabled by default for each joined access point, and access point authentication is automatically disabled. After MFP is globally enabled on a controller, you can disable and re-enable it for individual WLANs and access points.

If you click to enable MFP Frame Validation, three main functions are performed:

- **Management frame protection**—When management frame protection is enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing those receiving access points which were configured to detect MFP frames to report the discrepancy.

- **Management frame validation**—When management frame validation is enabled, the access point validates every management frame it receives from other access points in the network. When the originator is configured to transmit MFP frames, the access point ensures that the MIC IE is present and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE, it reports the discrepancy to the network management system. To report this discrepancy, the access point must have been configured to transmit MFP frames. Likewise, for the timestamps to operate properly, all controllers must be Network Transfer Protocol (NTP) synchronized.

- **Event reporting**—The access point notifies the controller when it detects an anomaly, and the controller aggregates the received anomaly events and reports the results through SNMP traps to alert the network manager.

**Step 15** Select the **Cisco Discovery Protocol** check box if you want to enable it. CDP is a device discovery protocol that runs on all Cisco-manufactured equipment, such as routers, bridges, and communication servers. Each device sends periodic messages to a multicast address and listens to the messages that others send to learn about neighboring devices. When the device boots, it sends a CDP packet specifying whether the device is inline power enabled so that the requested power can be supplied.

**Note** Changing access point parameters temporarily disables an access point and might result in loss of connectivity to some clients.

**Step 16** Select the check box to enable rogue detection.
Note: Rogue detection is disabled automatically for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. For more information regarding OfficeExtend access points, see the *Cisco Wireless LAN Controller Configuration Guide.*

**Step 17** Select the **Encryption** check box to enable encryption.

**Note:** Enabling or disabling encryption functionality causes the access point to reboot, which then causes clients to lose connectivity.

**Note:** DTLS data encryption is enabled automatically for OfficeExtend access points to maintain security, but disabled by default for all other access points.

**Note:** Cisco 5500 controllers can be loaded with one of the two types of images, AS_5500_LDPE_x_x_x_x.aes or AS_5500_x_x_x_x.aes. For the 5500 controller loaded with former image, you need to have DTLS License to show encryption.

**Note:** For WiSM2 and 2500 controllers, it is mandatory to have DTLS license to show encryption.

**Step 18** If rogue detection is enabled, the access point radio is turned off, and the access point listens to wired traffic only. The controllers that operate in this mode monitor the rogue access points. The controller sends all the rogue access point and client MAC address lists to the rogue detector, and the rogue detector forwards this information to the WLC. The MAC address list is compared to what the WLC access points expected. If the MAC addresses match, you can determine which rogue access points are connected on the wired network.

**Step 19** Select the **SSH Access** check box to enable SSH access.

**Step 20** Select the **Telnet Access** check box to enable Telnet access.

**Note:** An OfficeExtend access point might be connected directly to the WAN which allows external access if the default password is used by the access point. Therefore, Telnet and SSH access are disabled automatically for OfficeExtend access points.

**Step 21** If you want to override credentials for this access point, select the **Override Global Username Password** check box. You can then enter a new supplicant AP username, AP password, and Enable password that you want to assign for this access point.

**Note:** In the System > AP Username Password page, you can set global credentials for all access points to inherit as they join a controller. These established credentials appear in the lower right of the AP Parameters tab page.

The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.
Step 22 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received.

Step 23 You can now manipulate power injector settings through Prime Infrastructure without having to go directly to the controllers. In the Power Over Ethernet Settings section, select the check box to enable pre-standard or power injector state.

Pre-standard is chosen if the access point is powered by a high power Cisco switch; otherwise, it is disabled. If power injector state is selected, power injector options appear. The possible values are installed or override. If you choose override, you can either enter a MAC address or leave it empty so that it is supplied by WLC.

**Note** To determine which source of power is running Prime Infrastructure, choose **Monitor > Access Points**, click **Edit View**, and then choose and move POE Status to the View Information box. After you click **Submit**, the POE status appears in the last column. If the device is powered by an injector, the POE status appears as Not Applicable.

Step 24 Select the **Enable** check box to enable the following FlexConnect configurations:

**Note** FlexConnect settings cannot be changed when the access point is enabled.

- **OfficeExtend AP**—The default is Enabled.

**Note** Unselecting the check box simply disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point, but it does put the access point at risk because it becomes remotely deployed. If you want to clear the configuration of an access point and return it to factory default settings, click **Clear Config** at the bottom of the access point details page. If you want to clear only the personal SSID of the access point, click **Reset Personal SSID** at the bottom of the access point details page.

When you select Enabled for the OfficeExtend AP, a warning message provides the following information:

- Configuration changes that automatically occur. Encryption and Link Latency are enabled. Rogue Detection, SSH Access, and Telnet Access are disabled.

- A reminder to configure at least one primary, secondary, and tertiary controller (including name and IP address).

**Note** Typically, an access point first looks for the primary controller to join. After that, the controller tries the secondary and then the tertiary controller. If none of these controllers are configured, the access point switches to a default discovery mode in an attempt to join whatever controller it might find.

An OfficeExtend access point searches only for a primary, secondary, or tertiary controller to join. It does not look any further for a configured controller. Because of this, it is important that you configure at least one primary, secondary, or tertiary controller name and IP address.
A warning the enabling encryption causes the access point to reboot and causes clients to lose connectivity.

- Least Latency Controller Join—When enabled, the access point switches from a priority order search (primary, secondary, and then tertiary controller) to a search for the controller with the best latency measurement (least latency). The controller with the least latency provides the best performance.

**Note** The access point only performs this search once when it initially joins the controller. It does not recalculate the primary, secondary, and tertiary controllers latency measurements once joined to see if the measurements have changed.

- VLAN Support—When selected, enter the Native VLAN identifier. When Enable VLAN is selected, Prime Infrastructure displays locally switched VLANs. You can only edit a VLAN ID that is mapped to a WLAN ID.

- AP level VLAN ACL Mapping—This group box appears only for FlexConnect mode access points with VLAN support enabled. You can only edit the Ingress and Egress ACLs mapped to a VLAN ID.

**Note** The AP level VLAN ACL Mapping configuration is pushed to the access point, only when the VLAN IDs entered in Prime Infrastructure is available in the AP Level VLAN ACL Mapping section of the access point in the associated controller.

- Group level VLAN ACL Mapping—This group box appears only for FlexConnect mode access points with VLAN support enabled. You can view the Group level VLAN ACL mapping that you have specified under the ACL tab of the FlexConnect ACL groups.

- PreAuthentication ACL Mappings

  - Web-Authentication and Web-Policy ACLs—Click the **External WebAuthentication ACLs** link to view the WebAuth and Web Policy ACL mappings at access point level. The ACL Mappings page lists details of the WLAN ACL mappings and web policy ACLs.

**Step 25** Select the role of the mesh access point from the Role drop-down list. The default setting is MAP.

**Note** An access point in a mesh network functions as either a root access point (RAP) or mesh access point (MAP).

**Step 26** Enter the name of the bridge group to which the access point belongs. The name can have up to 10 characters.

**Note** Bridge groups are used to logically group the mesh access points to avoid two networks on the same channel from communicating with each other.

**Note** For mesh access points to communicate, they must have the same bridge group name.

**Note** For configurations with multiple RAPs, make sure that all RAPs have the same bridge group name to allow failover from one RAP to another.
### Access Point Radios

**Note**
For configurations where separate sectors are required, make sure that each RAP and its associated MAPs have separate bridge group names.

The Type field appears whether the mesh access point is an indoor or outdoor access point, and the Backhaul Interface field displays the access point radio that is being used as the backhaul for the access point.

**Step 27** Choose the data rate for the backhaul interface from the drop-down list. Data rates available are dictated by the backhaul interface. The default rate is 18 Mbps.

**Note**
This data rate is shared between the mesh access points and is fixed for the whole mesh network.

**Note**
Do NOT change the data rate for a deployed mesh networking solution.

**Step 28** Choose **Enable** from the Ethernet Bridging drop-down list to enable Ethernet bridging for the mesh access point.

**Step 29** Click **Save** to save the configuration.

**Step 30** Re-enable the access point radios.

**Step 31** If you need to reset this access point, click **Reset AP Now**.

**Step 32** Click **Reset Personal SSID** to reset the OfficeExtend access point personal SSID to the factory default.

**Step 33** If you need to clear the access point configuration and reset all values to the factory default, click **Clear Config**.

---

### Configuring an Ethernet Interface

**Note**
The 152x mesh access points are configured on any one of these four ports: port 0-PoE in, port 1-PoE out, Port 2 - cable, and port 3 - fiber. Other APs (such as 1130, 1140, 1240, 1250) are configured on Port 2 - cable.

To configure an Ethernet interface, follow these steps:

**Step 1** Choose **Configuration > Wireless Technologies > Access Point Radios**.

**Step 2** Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears.

**Note**
The Access Point Details page displays the list of Ethernet interfaces.

**Step 3** Click the link under Interface to see detailed information about that interface. The Ethernet Interface page appears.

This page displays the following parameters:
• AP Name—The name of the access point.
• Slot Id—Indicates the slot number.
• Admin Status—Indicates the administration state of the access point.
• CDP State—Select the CDP State check box to enable the CDP state.

Step 4 Click Save.

Importing AP Configuration

To import a current access point configuration file, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.
Step 2 From the Select a command drop-down list, choose Import AP Config.
A pop-up alert box appears stating All Unified AP(s) are imported from CSV file only. Unified AP(s) from Excel and XML file are not imported.
Step 3 Click OK to close the pop-up alert box.
Step 4 Click Go.
Step 5 Enter the CSV file path in the text box or click Browse to navigate to the CSV file on your computer.
The first row of the CSV file is used to describe the columns included. The AP Ethernet Mac Address column is mandatory. The parameters on this page are used for columns not defined in the CSV file.
Sample File Header:

AP Name, Ethernet MAC, Location, Primary Controller, Secondary Controller, Tertiary Controller
ap-1, 00:1c:58:74:8c:22, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3

The CSV file can contain following fields.
• AP Ethernet MAC Address—Mandatory
• AP Name—Optional
• Location—Optional
• Primary Controller—Optional
• Secondary Controller—Optional
• Tertiary Controller—Optional
Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.
• Ethernet MAC—AP Ethernet MAC Address
• AP Name—AP Name
• Location—AP Location
• Primary Controller—Primary Controller Name
• Secondary Controller—Secondary Controller Name
• Tertiary Controller—Tertiary Controller Name
Note: Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

Step 6: When the appropriate CSV file path appears in the Select CSV File text box, click OK.

Related Topics

- Configuring Access Point Details
- Configuring Access Points 802.11n Antenna
- Viewing Audit Status (for Access Points)
- Searching Access Points
- Copying and Replacing Access Points
- Removing Access Points
- Scheduling Radio Status
- Exporting AP Configuration
- Downloading Images to Autonomous Access Points (TFTP)

Exporting AP Configuration

To export current access point configuration files, follow these steps:

Step 1: Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2: From the Select a command drop-down list, choose Export AP Config.

A pop-up alert box appears stating All Unified AP(s) are exported to CSV/EXCEL/XML file.

Step 3: Click OK to close the pop-up alert box.

Step 4: Click Go to view the current AP configurations including:

- AP Name
- Ethernet MAC
- Location
- Primary Controller
- Secondary Controller
- Tertiary Controller

Step 5: Select the file option (CSV, Excel, XML) to export the access point configurations.

Step 6: In the File Download window, click Save to save the file.
Configuring Access Points 802.11n Antenna

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

**Note** At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

If you choose **Configuration > Wireless Technologies > Access Point Radios**, and select an 802.11n item from the Radio column, the following page appears.

This page contains the following fields:

**General**

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the base radio of the access point.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the **CDP State** check box to enable CDP.
- Controller—IP address of the controller. Click the IP address of the controller for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—Select the check box to enable CleanAir.

**Antenna**

- Antenna Type—Indicates an external or internal antenna.
- Antenna Diversity—Select **Right**, **Left**, or **Enabled**.

**Note** Antenna diversity refers to the Cisco Aironet access point feature where an access point samples the radio signal from two integrated antenna ports and chooses the preferred antenna. This diversity option is designed to create robustness in areas with multi-path distortion.

For external antenna, select one of the following:

- **Enabled**—Use this setting to enable diversity on both the left and right connectors of the access point.
- **Left**—Use this setting if your access point has removable antennas and you install a high-gain antenna on the left connector of the access point.
- **Right**—Use this setting if your access point has removable antennas and you install a high-gain antenna on the right connector of the access point.

For internal antennas, select one of the following:
- **Enabled**—Use this setting to enable diversity on both Side A and Side B.
- **Side A**—Use this setting to enable diversity on Side A (front antenna) only.
- **Side B**—Use this setting to enable diversity on Side B (rear antenna) only.

- **External Antenna**—Choose the **external antenna** or **Other** from the drop-down list.
- **Antenna Gain**—Enter the desired antenna gain in the text box.

**Note**
The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means $4 \times 0.5 = 2$ dBm of gain.

- **Current Gain (dBm)**—Indicates the current gain in dBm.

Table 29-1 lists the antenna names, gain, and descriptions.

<table>
<thead>
<tr>
<th>Antenna Name</th>
<th>Gain (dBi)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIR-ANT2450HG-N</td>
<td>5.0</td>
<td>Omni directional horizontal polarization antenna</td>
</tr>
<tr>
<td>AIR-ANT2450VG-N</td>
<td>5.0</td>
<td>Omni directional vertical polarization antenna</td>
</tr>
<tr>
<td>AIR-ANT5150HG-N</td>
<td>5.0</td>
<td>Omni directional horizontal polarization antenna</td>
</tr>
<tr>
<td>AIR-ANT5150VG-N</td>
<td>5.0</td>
<td>Omni directional vertical polarization antenna</td>
</tr>
<tr>
<td>AIR-ANT2524DB-R=</td>
<td>2/4</td>
<td>Dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2524DG-R=</td>
<td>2/4</td>
<td>Dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2524DW-R=</td>
<td>2/4</td>
<td>Dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2535SDW-R=</td>
<td>3/5</td>
<td>Dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2524V4C-R=</td>
<td>2/4</td>
<td>Omni ceiling antenna</td>
</tr>
<tr>
<td>AIR-ANT2566P4W-R=</td>
<td>6/6</td>
<td>Patch wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2544V4M-R=</td>
<td>4/4</td>
<td>Omni wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2544V4M-R8=</td>
<td>3/2</td>
<td>Omni wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2566D4M-R=</td>
<td>6/6</td>
<td>Directional wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2513P4M-N=</td>
<td>13/13</td>
<td>Patch wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT-LOC-01=</td>
<td></td>
<td>Omni antenna</td>
</tr>
<tr>
<td>AIR-ANT1000</td>
<td>0.00</td>
<td>AP 1000 Integrated antenna</td>
</tr>
<tr>
<td>CUSH-S5157WP</td>
<td>3.00</td>
<td>5.15-5.87 GHz diversity wideband panel antenna (side gain and back attenuation)</td>
</tr>
<tr>
<td>KODIAK-DIRECTIONAL</td>
<td>8.00</td>
<td>Integrated Kodiak directional antenna</td>
</tr>
<tr>
<td>KODIAK-OMNI</td>
<td>5.00</td>
<td>Kodiak omni antenna</td>
</tr>
<tr>
<td>AIR-ANT1728</td>
<td>5.20</td>
<td>Omni ceiling mount antenna</td>
</tr>
<tr>
<td>AIR-ANT1729</td>
<td>6.00</td>
<td>Patch wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2012</td>
<td>6.50</td>
<td>Diversity patch wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2410Y-R</td>
<td>10.00</td>
<td>Yagi master or wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT5959</td>
<td>2.00</td>
<td>Omni diversity ceiling mount antenna</td>
</tr>
</tbody>
</table>
### Table 29-1 Antenna Names, Gain, and Descriptions (continued)

<table>
<thead>
<tr>
<th>Antenna Name</th>
<th>Gain (dBi)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AJAX-OMNI</td>
<td>5.00</td>
<td>Integrated Ajax omni antenna</td>
</tr>
<tr>
<td>AIR-ANT5135D-R</td>
<td>3.50</td>
<td>Omni dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT5135DW-R</td>
<td>3.50</td>
<td>3.5-dBi white dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT5135DG-R</td>
<td>3.50</td>
<td>3.5 dB5 gray non-articulating dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2413P2M-N</td>
<td>13.00</td>
<td>Dual polarized patch antenna for 2.4 GHz.</td>
</tr>
<tr>
<td>AIR-ANT2422DW-R</td>
<td>2.20</td>
<td>2.2-dBi white dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2422DB-R</td>
<td>2.20</td>
<td>Omni dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2422DG-R</td>
<td>2.20</td>
<td>2.2 dBi gray non-articulating dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT5145V-R</td>
<td>4.50</td>
<td>Omni diversity antenna</td>
</tr>
<tr>
<td>AIR-ANT5160V-R</td>
<td>6.00</td>
<td>Omni antenna</td>
</tr>
<tr>
<td>AIR-ANT3549</td>
<td>9.00</td>
<td>Patch wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT4941</td>
<td>2.20</td>
<td>Omni dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2506</td>
<td>0.00</td>
<td>Omni mass mount antenna</td>
</tr>
<tr>
<td>AIR-ANT3213</td>
<td>5.20</td>
<td>Omni diversity pillar antenna</td>
</tr>
<tr>
<td>CUSH-S24516DBP</td>
<td>3.00</td>
<td>Integrated 2.4/5 GHz hemispheric pattern</td>
</tr>
<tr>
<td>CUSH-S5153WBPX</td>
<td>6.00</td>
<td>Ceiling mount 6-dBi omni</td>
</tr>
<tr>
<td>AIR-ANT5170V-R</td>
<td>7.00</td>
<td>Wall mount diversity patch antenna</td>
</tr>
<tr>
<td>AIR-ANT5175V</td>
<td>7.50</td>
<td>Omni antenna for Wireless Bridge</td>
</tr>
<tr>
<td>AIR-ANT5195V-R</td>
<td>9.50</td>
<td>Wall mount patch antenna</td>
</tr>
<tr>
<td>AIR-ANT58G10SSA</td>
<td>9.50</td>
<td>Sector antenna for Wireless Bridge</td>
</tr>
<tr>
<td>AIR-ANT2455V</td>
<td>5.50</td>
<td>Omni antenna for Wireless Bridge</td>
</tr>
<tr>
<td>CUSH-S54717P</td>
<td>17.00</td>
<td>Patch array antenna for Wireless Bridge</td>
</tr>
<tr>
<td>CUSH-S49014WP</td>
<td>14.00</td>
<td>Patch array antenna for Wireless Bridge</td>
</tr>
<tr>
<td>CUSH-S2406BP</td>
<td>8.00</td>
<td>Omni antenna for Wireless Bridge</td>
</tr>
<tr>
<td>AIR-ANT1100</td>
<td>2.20</td>
<td>Default antenna for AP1100</td>
</tr>
<tr>
<td>BR1310</td>
<td>13.00</td>
<td>Integrated patch directional antenna</td>
</tr>
<tr>
<td>AIR-ANT2460</td>
<td>6.00</td>
<td>Patch wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2465</td>
<td>6.50</td>
<td>Diversity patch wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2485</td>
<td>9.00</td>
<td>Patch wall mount antenna</td>
</tr>
<tr>
<td>AIR-ANT2480V-N</td>
<td>8.00</td>
<td>2.4 GHz omni antenna for mesh</td>
</tr>
<tr>
<td>AIR-ANT5114P2M-N</td>
<td>14.00</td>
<td>5 GHz patch for mesh</td>
</tr>
<tr>
<td>AIR-ANT5117S-N</td>
<td>17.00</td>
<td>5 GHz sector for mesh</td>
</tr>
<tr>
<td>AIR-ANT2450V-N</td>
<td>5.00</td>
<td>2.4 GHz omni antenna</td>
</tr>
<tr>
<td>AIR-ANT5180V-N</td>
<td>8.00</td>
<td>5 GHz omni antenna</td>
</tr>
<tr>
<td>AIR-ANT2450S-R</td>
<td>5.50</td>
<td>2.4 GHz 135-degree sector antenna</td>
</tr>
</tbody>
</table>
### Table 29-2  Access Point Radios

<table>
<thead>
<tr>
<th>Antenna Name</th>
<th>Gain (dBi)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIR-ANT2451V-R</td>
<td>2.4 GHz—2.0, 5 GHz—3.0</td>
<td>2.4 GHz and 5 GHz four-element dual band antenna. <strong>Note</strong> Two elements for the 2.4 GHz band and two elements for the 5 GHz band.</td>
</tr>
<tr>
<td>AIR-ANT2460NP-R</td>
<td>6.00</td>
<td>2.4 GHz MIMO (3-Element) Patch Antenna</td>
</tr>
<tr>
<td>AIR-ANT5160NP-R</td>
<td>6.00</td>
<td>5 GHz MIMO (3-Element) Patch Antenna</td>
</tr>
<tr>
<td>AIR-ANT2420V-N</td>
<td>2.2</td>
<td>Omni dipole antenna</td>
</tr>
<tr>
<td>AIR-ANT2422SDW-R</td>
<td>2.20</td>
<td>2.4 GHz “Stubby” white monopole antenna</td>
</tr>
<tr>
<td>AIR-ANT5135SDW-R</td>
<td>3.50</td>
<td>5 GHz “Stubby” white monopole antenna</td>
</tr>
<tr>
<td>AIR-ANT2451NV-R</td>
<td>2.4 GHz—2.5, 5 GHz—3.5</td>
<td>2.4 GHz and 5 GHz “6-pack” ceiling mount omni antenna</td>
</tr>
<tr>
<td>AIR-ANT2452V-R</td>
<td>5.2</td>
<td>2.4 GHz Diversity Wall Mount Omni-directional Antenna. <strong>Note</strong> This is a replacement antenna to the existing AIR-ANT3213.</td>
</tr>
<tr>
<td>AIR-ANT24020V-R</td>
<td>2.0</td>
<td>External omni diversity ceiling mount antenna. <strong>Note</strong> This is a replacement antenna to the existing antenna AIR-ANT5959.</td>
</tr>
<tr>
<td>AIR-ANT5140V-R</td>
<td>4.0</td>
<td>Omni antenna w/RP-TNC connectors(3)</td>
</tr>
<tr>
<td>AIR-ANT2430V-R</td>
<td>3.0</td>
<td>Omni antenna w/RP-TNC connectors(3)</td>
</tr>
<tr>
<td>AIR-ANT1949</td>
<td>2.4 GHz—13.5</td>
<td>External antenna</td>
</tr>
<tr>
<td>AIR-ANT2440NV-R</td>
<td>4.0</td>
<td>2.4 GHz MIMO Wall Mount Antenna</td>
</tr>
<tr>
<td>AIR-ANT5140NV-R</td>
<td>4.0</td>
<td>5 GHz MIMO Wall Mount Antenna</td>
</tr>
<tr>
<td>AIR-ANT2460P-R</td>
<td>6.0</td>
<td>Grayling Patch Antenna</td>
</tr>
<tr>
<td>AIR-ANT2485P-R</td>
<td>8.5</td>
<td>Grayling Patch Antenna</td>
</tr>
<tr>
<td>AIR-ANT2547V-N</td>
<td>2.4 GHz—4.0, 5 GHz—7.0</td>
<td>2.4 GHz and 5 GHz dual band Omni-directional Antenna.</td>
</tr>
<tr>
<td>AIR-ANT2588P3M-N</td>
<td>8.0</td>
<td>Dual-band patch antenna for both 2.4 GHz and 5 GHz.</td>
</tr>
<tr>
<td>Internal-802.11</td>
<td>2</td>
<td>Internal AP802 Antenna</td>
</tr>
<tr>
<td>Internal-602i</td>
<td>2.4 GHz—4</td>
<td>Internal omni antenna</td>
</tr>
<tr>
<td>Internal-602i</td>
<td>5.0 GHz—4</td>
<td>Internal omni antenna</td>
</tr>
</tbody>
</table>

*Table 29-2* lists the default values of some of the attributes of an access point when it is added to Prime Infrastructure for the first time.
<table>
<thead>
<tr>
<th>AP Type</th>
<th>Radio Type</th>
<th>Supported Antennas</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP 1131</td>
<td>802.11a</td>
<td>AJAX-OMNI</td>
</tr>
<tr>
<td></td>
<td>802.11b/g</td>
<td>AJAX-OMNI</td>
</tr>
<tr>
<td>AP 1100</td>
<td>802.11b/g (only b/g)</td>
<td>AIR-ANT1100</td>
</tr>
</tbody>
</table>
### Table 29-2  Supported Antennas (continued)

<table>
<thead>
<tr>
<th>AP Type</th>
<th>Radio Type</th>
<th>Supported Antennas</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b/g</td>
<td>AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R</td>
<td></td>
</tr>
<tr>
<td>802.11b/g</td>
<td>AIR-ANT1000, AIR-ANT4941, AIR-ANT1728, AIR-ANT2012, AIR-ANT1729, AIR-ANT5959, AIR-ANT2506, AIR-ANT3213, AIR-ANT2460, AIR-ANT2465, AIR-ANT2485, CUSH-S24516DBP, AIR-ANT2452V-R, AIR-ANT24020V-R</td>
<td></td>
</tr>
<tr>
<td>802.11a</td>
<td>AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP</td>
<td></td>
</tr>
<tr>
<td>802.11b/g</td>
<td>AIR-ANT2455V, CUSH-S2406BP</td>
<td></td>
</tr>
<tr>
<td>802.11a</td>
<td>AIR-ANT5175V, AIR-ANT58G10SSA, CUSH-S54717P, CUSH-S49014WP</td>
<td></td>
</tr>
<tr>
<td>802.11b/g</td>
<td>AIR-ANT2455V, CUSH-S2406BP</td>
<td></td>
</tr>
<tr>
<td>802.11a</td>
<td>AIR-ANT2455V, CUSH-S2406BP</td>
<td></td>
</tr>
<tr>
<td>AP Type</td>
<td>Radio Type</td>
<td>Supported Antennas</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>AP 1140</td>
<td>802.11b/g</td>
<td>Internal-1040-5.0 GHz</td>
</tr>
<tr>
<td>AP 1140</td>
<td>802.11b/g</td>
<td>Internal-1040-2.4 GHz</td>
</tr>
<tr>
<td>AP 1550</td>
<td>802.11a</td>
<td>AIR-ANT2547V-N-5.0GHz, Internal-1550-5.0 GHz</td>
</tr>
<tr>
<td>AP 1550</td>
<td>802.11b/g</td>
<td>AIR-ANT2547V-N-2.4GHz, Internal-1550-2.4GHz</td>
</tr>
<tr>
<td>AP2600E</td>
<td>802.11 a/n</td>
<td>AIR-ANT2524DB-R-5GHz</td>
</tr>
<tr>
<td>AP2600E</td>
<td>802.11b/g</td>
<td>AIR-ANT2524DB-R-2.4GHz</td>
</tr>
<tr>
<td>AP2600I</td>
<td>802.11 a/n</td>
<td>Internal-2600-5GHz</td>
</tr>
<tr>
<td>AP2600I</td>
<td>802.11b/g</td>
<td>Internal-2600-2.4GHz</td>
</tr>
<tr>
<td>AP 3500e</td>
<td>802.11a</td>
<td>Internal-3500i-5 GHz</td>
</tr>
<tr>
<td>AP 3500e</td>
<td>802.11b/g</td>
<td>Internal-3500i-2.4 GHz</td>
</tr>
<tr>
<td>AP 3600e</td>
<td>802.11b/g</td>
<td>AIR-ANT2524DB-R, AIR-ANT2524DW-R, AIR-ANT2524DG-R, AIR-ANT2566P4W-R, AIR-ANT2524V4C-R.</td>
</tr>
<tr>
<td>AP 3600i</td>
<td>802.11a</td>
<td>Internal-3600i-5 GHz</td>
</tr>
<tr>
<td>AP 3600i</td>
<td>802.11b/g</td>
<td>Internal-3600i-2.4 GHz</td>
</tr>
</tbody>
</table>
WLAN Override

The following 802.11a WLAN Override field appears:

- WLAN Override—Choose Enable or Disable from the drop-down list.

**Note** When you enable WLAN Override, operating system displays a table showing all current Cisco WLAN Solution WLANs. In the table, select WLANs to enable WLAN operation, and deselect WLANs to disallow WLAN operation for this 802.11a Cisco Radio.

**Note** WLAN override does not apply to access points that support the 512 WLAN feature.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- ClientLink—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.
Chapter 29      Configuring Wireless Technologies

Access Point Radios

Note

The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear:

- **Current Channel**—Channel number of the access point.
- **Assignment Method**—Select one of the following:
  - **Global**—Use this setting if the channel of the access point is set globally by the controller.
  - **Custom**—Use this setting if the channel of the access point is set locally. Select a channel from the drop-down list.

  For example, if you select 2(17 dBm) as the custom power, 2 corresponds to the Power Level and 17 is the Absolute Power (dBm).

- **Channel width**—Select the channel width from the drop-down list. The selections include 20, above 40, and below 40.

  RF Channel assignment supports 802.11n 40 MHz channel width in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates.

Note

Selecting a larger bandwidth reduces the non-overlapping channels which could potentially reduce the overall network throughput for certain deployments.

Note

The power level and channel numbers of an access point are not audited.

Tx Power Level Assignment

- **Current Tx Power Level**—Indicates the current transmit power level.
- **Assignment Method**—Select one of the following. When the XOR radio is in 5GHz, you can configure only **Global** assignment method.
  - **Global**—Use this setting if the power level is set globally by the controller.
  - **Custom**—Use this setting if the power level of the access point is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note

At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

Select any of the 11n Antenna Selection parameters:

- **Antenna A**
Access Point Radios

Chapter 29      Configuring Wireless Technologies

11n Parameters

The following 11n fields appear:

- 11n Supported—Indicates whether or not 802.11n radios are supported.
- Client Link—Use this option to enable or disable client links. Choose Enable, Disable, or Not Applicable from the drop-down list.

Configuring CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note
CDP is enabled on the Ethernet and radio ports of the bridge by default.

Configuring CDP on Access Points

To configure CDP on Radio or Ethernet interfaces, follow these steps:

Step 1  Choose Configuration > Wireless Technologies > Access Point Radios.
Step 2  Choose an access point associated with software release 5.0 or later.
Step 3  Click the slots of radio or an Ethernet interface for which you want to enable CDP.
Step 4  Select the CDP State check box to enable CDP on the interface.
Step 5  Click Save.

Configuring Access Points XOR Antenna

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

If you choose Configuration > Wireless Technologies > Access Point Radios, and select an XOR (2.4GHz) or XOR(5GHz) from the Radio column, the following page appears.

This page contains the following fields:

Note
Changing any of the fields causes the radio to be temporarily disabled and thus might result in loss of connectivity for some clients.
General

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the base radio of the access point.
- Slot ID—Slot ID.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the CDP State check box to enable CDP.
- Controller—IP address of the controller. Click the IP address of the controller for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—From the drop-down choose any of the options: Both Disabled, 5GHz Enabled, 2.4 GHz Enabled, and Both Enabled.

Radio Assignment

- Assignment Method—The assignment methods are: Auto, Serving, or Monitor.

Note

Band Selection, RF Channel Assignment, and Tx Power Level Assignment appears only for Serving assignment method.

- Band Selection—You can either choose 2.4 GHz or 5 GHz radio.

Antenna

Depending on the Radio Assignment selection, the following parameters appear:

- Antenna Type—Indicates the antenna type: External or Internal.
- XOR A Antenna—(Displayed only for Auto assignment method). Choose the external antenna or Other from the drop-down list.
- XOR B Antenna—(Displayed only for Auto assignment method). Choose the external antenna or Other from the drop-down list.
- External Antenna—(Displayed for Serving and Monitor assignment method). Choose the external antenna or Other from the drop-down list. The values in the drop-down varies for 2.4 GHz and 5GHz radio.
- Antenna Gain—(Displayed for Serving and Monitor assignment method.) Enter the desired antenna gain in the text box. To configure the custom antenna gain, select Others for the External Antenna option.

Note

The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear only if you have selected Radio Assignment method as Serving.
Access Point Radios

- **Current Channel**—Channel number of the access point.
- **Channel Width**—Only radios with 20 MHz is supported for a 2.4 GHz radio. For a 5 GHz radio, from the Channel Width drop-down list, choose 20 MHz, 40 MHz, 80 MHz or 160 MHZ.
- **Assignment Method**—Select one of the following:
  - **Global**—Use this setting if the channel of the access point is set globally by the controller.
  - **Custom**—Use this setting if the channel of the access point is set locally. Select a channel from the **Custom** drop-down list. The values in the drop-down varies for 2.4 GHz and 5 GHz radios.

11n and 11ac Parameters

- **11n Supported**—Indicates whether or not 11n radio is supported.
- **11ac Supported**—Indicates whether or not 11ac radio is supported.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- **ClientLink**—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

  **Note**  The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

Tx Power Level Assignment

- **Current Tx Power Level**—Indicates the current transmit power level.
- **Assignment Method**—Select one of the following. When the XOR radio is in 5GHz, you can configure only **Global** assignment method.
  - **Global**—Use this setting if the power level is set globally by the controller.
  - **Custom**—Use this setting if the power level of the access point is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

  **Note**  At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

Select any of the 11n Antenna Selection parameters:

- **Antenna A**
- **Antenna B**
- **Antenna C**
Chapter 29  Configuring Wireless Technologies

Access Point Radios

11n Parameters

The following 11n fields appear:

- 11n Supported—Indicates whether or not 802.11n radios are supported.
- Client Link—Use this option to enable or disable client links. Choose Enable, Disable, or Not Applicable from the drop-down list.

Configuring Access Point Radios for Tracking Optimized Monitor Mode

To optimize monitoring and location calculation of tags, you can enable Tracking Optimized Monitor Mode (TOMM) on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

After enabling Monitor mode at the access point level, you must then enable TOMM and assign monitoring channels on the 802.11b/g radio of the access point.

Note

For details on enabling Monitor mode on an access point, see Step 6 in the “Configuring Access Point Details” section on page 29-xii.

To set enable TOMM and assign monitoring channels on the access point radio, follow these steps:

Step 1
After enabling Monitor mode at the access point level, choose Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2
In the Access Points page, click the 802.11 b/g Radio link for the appropriate access point.

Step 3
In the General group box, disable Admin Status by unselecting the check box. This disables the radio.

Step 4
Select the TOMM check box. This check box only appears for Monitor Mode APs. The drop-down lists for each of the four configurable channels are displayed.

Step 5
Choose the four channels on which you want the access point to monitor tags.

Note
You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, choose None from the channel drop-down list.

Step 6
Click Save. Channel selection is saved.

Step 7
In the Radio parameters page, reenable the radio by selecting the Admin Status check box.

Step 8
Click Save. The access point is now configured as a TOMM access point.

The AP Mode displays as Monitor/TOMM in the Monitor > Access Points page.
Copy and Replacing Access Points

The Copy and Replace AP feature is useful if you need to remove an access point from the network and replace it with a new access point. All of the access point information, such as AP mode, name, and map location needs to be copied from the old access point to the new access point.

To access the Copy and Replace AP function, follow these steps:

2. Select the check box for the applicable access point.
3. From the Select a command drop-down list, choose Copy and Replace AP.
4. Click Go.

The old access point needs to be removed from the network first. This access point then becomes unassociated to any controller. When you plug in the new access point, it is associated with the controller and Prime Infrastructure refreshes the information. At that point, select the old unassociated access point and choose to copy and replace the configuration to the new access point.

Note
If a different access point type is used to replace an older access point, only the configuration parameters that apply are copied.

Bulk Copy and Replacing the Access Points

Using the Bulk Copy and Replace AP feature, you can remove hundreds of access points from the network and replace them with the new access points. The access point information such as, AP Mode, AP Name, and MAC Address is copied from the old access points to the new access points.

1. Physically replacing the APs:
   - Ensure that the access points that were associated with the Cisco WLC is already managed by the Cisco Prime Infrastructure.
   - Identify the APs that need to be replaced.
   - Older 802.11n APs are physically replaced with the newer 802.11ac APs.
   - Note down the Name and MAC address of the 802.11n and 802.11ac APs.
   - Update the CSV file with the new Name and MAC Address.

2. Refresh the Cisco WLC configurations on Cisco Prime Infrastructure:
   - After replacing the APs physically, refresh the WLC configurations on the Cisco Prime Infrastructure.
   - Ensure the Lightweight Operational Status Background task is running or enabled.
   - Go to Configure > Controller > Access Points to check if the new 802.11ac APs are displaying and the old 802.11n APs status is displayed as Not Associated.

3. Perform Bulk Copy Replace on the Cisco Prime Infrastructure. To perform bulk copy and replace AP, follow these steps:

   2. From the Select a command drop-down list, choose bulk Copy and Replace AP, click Go.
### Configuring Wireless Technologies

**Access Point Radios**

#### Step 3
Click Choose File to select CSV file, and then find the location of the CSV file that you want to import.

#### Step 4
Click OK.

---

### Removing Access Points

To remove access points that are not associated, follow these steps:

**Step 1**
Choose **Configuration > Wireless Technologies > Access Point Radios**.

**Step 2**
From the Select a command drop-down list, choose **Remove APs**.

**Step 3**
Click **Go**.

**Step 4**
Click **OK** to confirm the removal.

---

### Scheduling and Viewing Radio Status

This section contains the following topics:

- [Scheduling Radio Status](#), page 29-xxxvii
- [Viewing Scheduled Tasks](#), page 29-xxxvii

#### Scheduling Radio Status

To schedule a radio status change (enable or disable), follow these steps:

**Step 1**
Choose **Configure > Access Points**.

**Step 2**
Select the check box for the applicable access point(s).

**Step 3**
From the Select a command drop-down list, choose **Schedule Radio Status**.

**Step 4**
Click **Go**.

**Step 5**
Choose **Enable** or **Disable** from the Admin Status drop-down list.

**Step 6**
Use the Hours and Minutes drop-down lists to determine the scheduled time.

**Step 7**
Click the calendar icon to select the scheduled date for the status change.

**Step 8**
If the scheduled task is recurring, choose **Daily** or **Weekly**, as applicable. If the scheduled task is a one-time event, choose **No Recurrence**.

**Step 9**
Choose **Save** to confirm the scheduled task.

---

#### Viewing Scheduled Tasks

To view currently scheduled radio status tasks, follow these steps:
**Step 1** Choose **Configure > Access Points**.

**Step 2** Select the check box for the applicable access point(s).

**Step 3** From the Select a command drop-down list, choose **View Scheduled Radio Task(s)**.

**Step 4** Click **Go**.

The Scheduled Task(s) information includes:
- Scheduled Task(s)—Choose the task to view its access points and access point radios.
- Scheduled Radio adminStatus—Indicates the status change (Enable or Disable).
- Schedule Time—Indicates the time the schedule task occurs.
- Execution status—Indicates whether or not the task is scheduled.
- Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.
- Next Execution—Indicates the time and date of the next task occurrence.
- Last Execution—Indicates the time and date of the last task occurrence.
- Unschedule—Click **Unschedule** to cancel the scheduled task. Click **OK** to confirm the cancellation.

---

**Viewing Audit Status (for Access Points)**

An Audit Status column in the Configure > Access Points page shows an audit status for each of the access points. You can also view the audit report for the selected access points. The report shows the time of the audit, the IP address of the selected access point, and the synchronization status.

To view the audit status, follow these steps:

**Step 1** Choose **Configure > Access Points**.

**Step 2** Click the **Audit Status** column value to go to the latest audit details page for the selected access point. This report is interactive and per access point.

**Note** If you hover your mouse cursor over the Audit Status column value, the time of the last audit is displayed.

To run an access point on-demand audit report, select the desired access point for which you want to run the report and choose **Audit Now** from the Select a command drop-down list. In versions prior to 4.1, the audit only spanned the parameters present in the AP Details and AP Interface Details page. In Release 4.1, this audit report covers complete access point level auditing. The audit results are stored in the database so that you can view the latest audit reports without having to run another audit.

**Note** The audit can only be run on an access point that is associated to a controller.
Filtering Alarms for Maintenance Mode Access Points

Prime Infrastructure uses critical alarms to track if the managed access points are down. The controller sends three different alarms when the following occurs:

- The Access point is down
- Radio A of the access point is down
- Radio B/G of the access point is down

In Release 7.0.172.0 and later, these 3 alarms are grouped into a single alarm.

When an access point is under technical maintenance, the critical alarms need to be deprioritized. You can deprioritize the severity of an alarm of an access point using the Configure > Access Points page. When you move an access point to maintenance state, the alarm status for that access point appears in black color.

This section contains of the following topics:

- Placing an Access Point in Maintenance State, page 29-xxxix
- Removing an Access Point from Maintenance State, page 29-xxxix

Placing an Access Point in Maintenance State

To move an access point to the maintenance state, follow these steps:

**Step 1** Choose **Prime Infrastructure > Configure > Access Points**.  
The Access Points page appears.

**Step 2** From the drop-down list, choose **Place in Maintenance State**, and click **Go**.  
The access point is moved to maintenance state.

Once the access point is moved to maintenance state, the access point down alarms are processed with lower severity instead of critical.

Removing an Access Point from Maintenance State

To remove an access point from the maintenance state, follow these steps:

**Step 1** Choose **Prime Infrastructure > Configure > Access Points**.  
The Access Points page appears.

**Step 2** From the drop-down list, choose **Remove from Maintenance State**, and click **Go**.  
The access point is removed from the maintenance state.

Searching Access Points

Use the search options in the uppermost right corner of the page to create and save custom searches:
• New Search: Enter an IP address, name, SSID, or MAC, and click Search.
• Saved Searches: Click Saved Search to choose a category, a saved custom search, or choose other criteria for a search from the drop-down lists.
• Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.

After you click Go, the access point search results appear (see Table 29-3).

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the access point.</td>
</tr>
<tr>
<td>Ethernet MAC</td>
<td>MAC address of the access point.</td>
</tr>
<tr>
<td>AP Name</td>
<td>Name assigned to the access point. Click the access point name item to display details.</td>
</tr>
<tr>
<td>Radio</td>
<td>Protocol of the access point is either 802.11a/n or 802.11b/g/n.</td>
</tr>
<tr>
<td>Map Location</td>
<td>Campus, building, and floor location.</td>
</tr>
<tr>
<td>Controller</td>
<td>IP address of the controller.</td>
</tr>
<tr>
<td>AP Type</td>
<td>Access point radio frequency type.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Displays the operational status of the Cisco radios (Up or Down).</td>
</tr>
<tr>
<td>Alarm Status</td>
<td>Alarms are color coded as follows:</td>
</tr>
<tr>
<td></td>
<td>• Clear = No Alarm</td>
</tr>
<tr>
<td></td>
<td>• Red = Critical Alarm</td>
</tr>
<tr>
<td></td>
<td>• Orange = Major Alarm</td>
</tr>
<tr>
<td></td>
<td>• Yellow = Minor Alarm</td>
</tr>
<tr>
<td>Audit Status</td>
<td>The audit status of the access point.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the access point.</td>
</tr>
<tr>
<td>AP Mode</td>
<td>Describes the role of the access point modes such as Local, FlexConnect, Monitor, Rogue Detector, Sniffer, Bridge, or SE-Connect.</td>
</tr>
</tbody>
</table>

Viewing Mesh Link Details

You can access mesh link details in several ways:
• Click the Mesh dashboard in Prime Infrastructure home page
• Choose Monitor > Access Points, click the Mesh Links tab and then click the Details link
• After you import a KML file from Google Earth, click the AP Mesh link

The current statistics are displayed at the top of the page followed by diagrams for certain statistics.
• SNR Graph—SNR Up and Down graphs are combined into one graph. Each set of data is represented by different colors.
• Link Metrics Graph—The Adjusted Link Metric and Unadjusted Link Metric is combined into one graph. Each set of data is represented by different colors.
• Packet Error Rate Graph—Displays the packet error rates in a graph.
• Link Events—The last five events for the link are displayed.
• Mesh Worst SNR Links—Displays the worst signal-to-noise ratio (SNR) links.
• AP Uptime—These statistics help determine if an access point is rebooting frequently.
• LWAPP Join Taken Time—These statistics determine how long it takes an access point to join.
• Location Links—Allows you to navigate to Prime Infrastructure map or the Google Earth location.

### Viewing or Editing Rogue Access Point Rules

You can view or edit current rogue access point rules on a single WLC. To access the rogue access point rules, follow these steps:

1. **Step 1** Choose Configure > Controllers.
2. **Step 2** Click an IP address in the IP Address column.
3. **Step 3** From the left sidebar menu, choose Security > Rogue AP Rules. The Rogue AP Rules displays the rogue access point rules, the rule types (malicious or friendly), and the rule sequence.
4. **Step 4** Choose a Rogue AP Rule to view or edit its details.

### Wireless Configuration Groups [Beta]

Wireless Configuration Groups [Beta] workflow is the improved workflow of WLAN Controller Configuration Groups feature, which is available in the Prime Infrastructure. With the improved Wireless Configuration workflow, you can:

• Select device specific templates.
• Deploy multiple templates on multiple devices.
• Audit multiple wireless templates from PI.

**Note**

Dependency templates do not work in this workflow.

**Related Topic**

• Creating a New Configuration Group
• Adding or Removing Templates from Wireless Configuration Group
• Auditing Wireless Configuration Groups
Creating a New Configuration Group

**Step 1** Choose **Configuration > Wireless Technologies > Wireless Configuration Groups [Beta]**.

**Step 2** Click **Create** to create a new configuration group.

The Configuration Group Workflow wizard appears.

**Step 3** In the **General Configuration** tab, enter the configuration group name, and click **Next**.

The Select Template tab appears.

**Step 4** In the Select Template tab, select the Device Type: **CUWN** or **CUWN-IOS**.

**Step 5** Drag and drop a template or a group from **Templates** tree view > **My Templates** to the **Selected Template(s)** group box.

The Selected Template(s) group box lists templates or groups, which were added from the Templates tree view.

**Step 6** Click **Save and Quit** to save the configuration group and quit the work flow.

**Step 7** Click **Next** to save the configuration group and to deploy the templates selected.

The Select Devices tab appears.

**Step 8** The Select Devices tab lists Controllers based on the device type selected.

**Step 9** Select the **Device Name** check box and click **Deploy**.

Once the deploy is successful, the Wireless Configuration Groups list page appears.

The Wireless Configuration Groups page contains the following details for the deployed device:

- Group Name
- Deployed Devices Count
- Templates Count
- Last Modified On
- Last Applied On
- Deploy Status
  - Not Initiated — Indicates if the device is deployed on any of the devices or not.
  - Success — Indicates the number of successful templates associated with the applicable IP address.
  - Partial Success / Failure — Indicates the number of failures with provisioning of templates to the applicable controller. Click on **Partial Success / Failure** link to know the reason for failure.

Auditing Wireless Configuration Groups

The Config Groups Audit page allows you to verify if the controllers configuration complies with the group template. During the audit, you can leave this screen or logout of Cisco Prime Infrastructure. The process continues, and you can return to this page later to view the report.

**Note**

Do not perform any other configuration group functions during the audit verification.
Configuring WLAN Controller Auto Provisioning

Prime Infrastructure simplifies WLAN deployments with support for auto-provisioning. Auto provisioning allows Prime Infrastructure to automatically configure a new or replace a current Cisco Wireless LAN Controller (WLC). Prime Infrastructure auto provisioning feature can simplify deployments for customers with a large number of controllers.

For Auto Provision to complete successfully so that Cisco Prime Infrastructure manages Cisco WLC, the Cisco WLC needs to send a COLD_START trap to the trap receiver (Prime Infrastructure). Prime infrastructure on receiving this trap checks if the device is marked for auto provision. If the device is marked for auto provision, it adds that device to Prime infrastructure and manages it.
The controller radio and b/g networks are initially disabled by the Prime Infrastructure startup configuration file. You can turn on those radio networks by using a template, which should be included as one of the automated templates.

**Related Topics**

- Adding an Auto Provisioning Filter
- Auto Provisioning Primary Search Key Settings

The Auto Provision Filters page allows you to create and edit auto provisioning filters that define the list of allowable devices to be auto provisioned or auto monitored by Prime Infrastructure.

For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status. To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration > Users, Roles, & AAA > User Groups > group name > List of Tasks Permitted in Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

Filter parameters include:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Identifies the name of the filter.</td>
</tr>
<tr>
<td>Filter Enable</td>
<td>Indicates whether or not the filter is enabled. Only enabled filters can participate in the Auto Provisioning process.</td>
</tr>
<tr>
<td>Monitor Only</td>
<td>If selected, the Cisco WLC defined in this filter is managed by Prime Infrastructure but not configured by Prime Infrastructure if the Cisco WLC contacts Prime Infrastructure during the auto provisioning process.</td>
</tr>
<tr>
<td>Filter Mode</td>
<td>Indicates the search mode for this filter (Host Name, MAC Address, or Serial Number).</td>
</tr>
<tr>
<td>Config Group Name</td>
<td>Indicates the Configuration Group name. All Config-Groups used by auto provision filters should not have any controller defined in them.</td>
</tr>
</tbody>
</table>

**Adding an Auto Provisioning Filter**

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To add an Auto Provisioning Filter:

**Step 1** Choose Configuration > Wireless Technologies > WLAN Controller Auto Provisioning.

**Step 2** Choose Add Filter from the Select a command drop-down list, then click Go.

**Step 3** Enter the required parameters.

You can specify the Dynamic Interface configuration and Device Specific configuration details only when you input a CSV file. These two configurations cannot be performed using the graphical user interface.

**Step 4** Click Save.
To change the default username and password, you need to delete and then recreate the admin user and explained in Steps 5 through Step 8.

**Step 5**  
To change the default username and password, you need to create a new read/write user on the controller using the Local Management User Template. You must create this new user so that you can delete the default admin user as shown in Step 6.

**Step 6**  
Choose **Inventory > Device Management > Network Devices > All Devices**, click on the controller name, click the **Configuration** tab, then select **Management > Local Management User**, select the admin user, then from the **Select a command** drop-down list, select **Delete Local Management User** and click **Go**.

**Step 7**  
Create a new admin user on the controller using the Local Management User Template.

**Step 8**  
Delete the user you created in Step 5.

---

**Related Topic**
- [Controller > Management > Local Management User](#)

---

**Auto Provisioning Primary Search Key Settings**

Use the Primary Search Key Setting to set the matching criteria search order.

**Step 1**  
Choose **Configuration > Plug and Play > Controller Auto Provisioning**, then from the left sidebar menu, choose **Setting**.

**Step 2**  
Click to highlight the applicable search key, then use the **Move Up** or **Move Down** buttons to move the search key to a higher or lower priority.

**Step 3**  
Click **Save** to confirm the changes.
Scheduling Configuration Tasks

- Managing AP Template Tasks
- Viewing WLAN Configuration Scheduled Task Results
- Managing Software Downloads

Managing Scheduled Configuration Tasks

The Scheduled Configuration Tasks page allows you to navigate to any templates, configuration tasks, or software download tasks that have been scheduled earlier and provides a filtered view of these tasks. This page displays the summary information about a task. The information includes the template name, last time the task was run, next time the task is scheduled to run, and a link to view the results of previous runs. You can also edit the template, modify the schedule, enable, disable, or delete a scheduled task.

After you create and schedule a configuration template, configuration group, or a software download task, the scheduled task or template is listed in the Scheduled Configuration Tasks page.

You cannot create any new scheduled task or template in this page. You can only edit the scheduled task or template that is already created.

You can modify, enable, disable, or delete the following scheduled configuration tasks:
- AP Template
- Configuration Group
- WLAN Configuration
- Download Software

Managing AP Template Tasks

The AP Template Tasks page allows you to manage current access point template tasks.

Before You Begin
At least one lightweight access point task must exist (see Creating Lightweight AP Configuration Templates).

To modify a current access point template task:

Step 1 Choose Configuration > Scheduled Configuration Task.
Managing Scheduled Configuration Tasks

Step 2 Select the template name of the applicable task.
Step 3 In the AP Radio/Template page, click the Apply/Schedule tab.
Step 4 Make any necessary changes to the current schedule or access point template, and click Schedule.

To enable a current access point template task:

Step 1 Choose Configuration > Scheduled Configuration Task.
Step 2 Select the check box of the scheduled task to be enabled.
Step 3 Choose Enable Schedule from the Select a command drop-down list, then click Go.

Related Topics
- Managing Scheduled Configuration Tasks
- Managing AP Template Tasks
- Viewing WLAN Configuration Scheduled Task Results

Viewing WLAN Configuration Scheduled Task Results

To view and manage all scheduled WLAN tasks in Cisco Prime Infrastructure:

Step 1 Choose Configuration > Scheduled Configuration Task.
Step 2 From the left sidebar menu, choose WLAN Configuration.
Step 3 Select the Task Name link to open the WLAN Schedule Detail page. In this page, you can modify the date and time of the scheduled task.
Step 4 Select the check box of the scheduled task and use the Select a command drop-down list to enable, disable, or delete selected tasks.

Related Topics
- Managing Scheduled Configuration Tasks
- Managing AP Template Tasks

Managing Software Downloads

Use this feature to manage the software download tasks.

- Adding a Download Software Task
- Modifying a Download Software Task
- Selecting Controllers for the Download Software Task
Adding a Download Software Task

To add a download software task:

**Step 1** Choose **Configuration > Scheduled Configuration Task**, then from the left sidebar menu, choose **Download Software**.

**Step 2** Choose **Add Download Software Task** from the **Select a command** drop-down list, then click **Go**.

**Step 3** Configure the following information:

- **General**
  - Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.

- **Schedule Details**
  - Download Type—Select the download type. Select the **Download software to controller** check box to schedule download software to controller or select the **Pre-download software APs** check box to schedule the pre-download software APs. If you select Download software to controller, specify the image details.

  **Note** The pre-download option is displayed only when all selected controllers are using the Release 7.0.x.x or later.

  To see Image Predownload status per AP, enable the task in the **Administration > Dashboards > Job Dashboard > System Jobs > Wireless Poller > AP Image Pre-Download Status**, and run an AP Image Predownload report from the Report Launch Pad.

  - Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

  **Note** Reboot Type Automatic can be set only when the **Download software to controller** option is selected.

  - Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Select the time from the hours and minutes drop-down lists.

  - Reboot date/time—This option appears only if select the reboot type “Scheduled”. Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

  Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download.

  If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller does not reboot. In such a case, wait for the pre-download to finish for all of the APs and reboot the controller manually.

  - Notification (Optional)—Enter the email address of recipient to send notifications via email.

  To receive email notifications, configure Prime Infrastructure mail server in the **Administration > Settings > Mail Server Configuration** page.

- **Image Details**—Specify the TFTP or FTP Server Information:

  Complete these details if you selected the Download software to controller option in Schedule Details area.
Managing Scheduled Configuration Tasks

TFTP—Specify the TFTP Server Information:
- From the File is Located on drop-down list, choose Local machine or TFTP server.
  If you choose TFTP server, choose Default Server or add a New server from the Server Name drop-down list.
- Specify the IP address of the TFTP server. This is automatically populated if the default server is selected.
- Specify the local filename or click Browse to navigate to the appropriate file.
- If you selected TFTP server previously, specify the filename.

FTP—Specify the FTP Server Information:
- FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button.
- From the File is Located on drop-down list, choose Local machine or FTP server.
  If you choose FTP server, choose Default Server or add a New server from the Server Name drop-down list.
- Specify the IP address of the FTP server. This is automatically populated if the default server is selected.
- Specify the local filename, or click Browse to navigate to the appropriate file.
- If you selected FTP server previously, specify the filename.

Step 4 Click Save.

Modifying a Download Software Task

Before You Begin
At least one download software task must exist (see Adding a Download Software Task).
To modify a download software task:

Step 1 Choose Configuration > Scheduled Configuration Task.
Step 2 From the left sidebar menu, choose Download Software.
Step 3 Click the Task Name link to open the Download Software Task page, make any changes, then click Save.
Any changes in Download Type (Download/Pre-download) or Server Type (FTP/TFTP) for the task in Enabled state sets the task to Disabled state, and all existing controllers are disassociated from the task.

Selecting Controllers for the Download Software Task

This page lists all the supported controllers that can be selected for the scheduled image download/pre-download task.
To select a controller for scheduled image download:

Step 1 Choose Configuration > Scheduled Configuration Task.
Step 2  From the left sidebar menu, choose **Download Software**.

Step 3  Click the Controller to open the Download Software Task details page, then click **Select Controller** to view the controller list.

**Note**  If the pre-download option is chosen for the task, then only the controllers with software Release 7.0.x.x or later are listed.

The Select Controllers page can also be accessed by choosing **Configuration > Scheduled Configuration Task > Download Software**, then clicking the hyperlink in the Select Controller column for any download task that is in the Enabled, Disabled or Expired state.

You cannot download software to any controllers with the Reachability Status of **Unreachable**.

Step 4  Make any necessary changes, then click **Save**.
Auditing Device Configurations to Ensure Compliance

Prime Infrastructure allows you to define device configuration baselines and audit policies so you can find and correct any configuration deviations in your network devices. You can schedule a compliance audit against multiple configuration files and get an audit report that indicates if any configurations deviate from the specified baseline.

To perform a compliance audit against the devices in your network, complete the following steps:

1. Complete the prerequisites for Compliance Services.
2. Define a compliance policy, which includes rules, conditions, and fixes.
3. Group policies into policy profiles.
4. Run the policy against the specified device(s), either immediately or at a specified time.
   Prime Infrastructure compares the device’s running configuration, or any show commands, with the content specified in the policy, detects any violations, and creates a report.
5. View the audit compliance report to view and fix any violations.

Related Topics
- Compliance Auditing Prerequisites
- Creating Compliance Policies
- Grouping Policies into Compliance Profiles
- Running Compliance Profiles Against Devices
- Viewing Compliance Audit Results
- Fixing Compliance Violations on Devices
Compliance Auditing Prerequisites

The Compliance Services feature is disabled by default. In order for you to use it, a Prime Infrastructure user with Administrator privileges must enable the feature. For details, see “Enabling Compliance Services” in Related Topics.

Please note that the Compliance Services feature is available only on the following Prime Infrastructure server options:

- The Professional virtual appliance. For details, see “Virtual Appliance Options” and “Understanding System Requirements” in Related Topics.
- The Cisco Unified Computing System (UCS) Gen 2 physical appliance. For details, see “Virtual Appliance Options” and “Understanding System Requirements” in Related Topics.
- Standard Prime Infrastructure virtual appliance. For details, see “Virtual Appliance Options” and “Understanding System Requirements” in Related Topics.

You cannot use Compliance Services on Express or Express-Plus Prime Infrastructure virtual appliances.

Related Topics

- Enabling Compliance Services
- Virtual Appliance Options
- Physical Appliance Options
- Understanding System Requirements
- Creating Compliance Policies

Creating Compliance Policies

A compliance policy is a set of CLI commands that define a desired baseline or expected configuration.

Step 1 Choose Configuration > Compliance > Policies.
Step 2 Click the Create Compliance Policy icon.
Step 3 Enter a title and description, then click Create.

You can now create policy rules for the policy.

To duplicate the policy click the i icon and choose Duplicate Policy.

Related Topics

- Compliance Auditing Prerequisites
- Creating Compliance Policy Rules
Creating Compliance Policy Rules

After you create a compliance policy, you must specify rules within the policy and define the conditions and the relevant fixes for any violations. Rules are platform-specific. Each policy must contain at least one rule; however, there is no limitation on the number of rules you can define for a policy.

Step 1  Choose Configuration > Compliance > Policies.
Step 2  From the left navigation pane, select the policy to which you want to add rules.
Step 3  From the work area pane, click New. A New Rule window opens.
Step 4  Complete the required information in the Rule Information, Platform Selection, Rule Inputs and Conditions and Actions areas. See Table 31-1 for field descriptions.


Step 5  Click Create.
Step 6  To duplicate an existing rule and add it to a policy, select the rule, then click Duplicate.
Step 7  Enter the appropriate fields, then click Save.

After you complete adding rules to the policy, you must create a profile. See Creating Compliance Policies.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>All information entered in this section is free text and does not impact the conditions and the subsequent violations.</td>
</tr>
<tr>
<td>Rule Title</td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a brief description</td>
</tr>
<tr>
<td>Impact</td>
<td>Enter a brief note on the impact of the violation that the rule will generate.</td>
</tr>
<tr>
<td>Suggested Fix</td>
<td>Enter a brief description of the fix that will help you decide to choose or to not choose the rule against a specific policy. This description appears when you check the rule in the Rule Selector pane.</td>
</tr>
</tbody>
</table>

Platform Selection

| Available Platforms   | Check the platforms on which the condition must be run. If you select Cisco Devices, all of Cisco platforms specified in the list are included. The platforms checked in this section impacts the ignore count of an audit job. For example, if you run a rule on all the devices within your scope, including devices not selected in the Available Platforms pane, such devices are not audited and are marked against Ignore count. |

Note: Cisco Prime Infrastructure 3.1 supports audit for AireOS Wireless LAN Controllers platform.
Creating Compliance Policies

Chapter 31 Auditing Device Configurations to Ensure Compliance

Table 31-1 Configuration > Compliance > Policies > New Rule Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule Inputs</strong></td>
<td></td>
</tr>
<tr>
<td>New Rule Input</td>
<td>Click New to add inputs for the new rule. The input you create in this pane reflects in the Policy Profile page. You must provide rule inputs for the rule you have selected. For example, you can create an input to be IP Address. Any user who wants to run this rule can enter an IP address specific to the rule and add it to a specific profile. Enter the required details: For Identifier, Enter your own Identifier, or click the Generate button to generate an identifier based on the title. The following fields appear based on the option that you choose in the Data Type field:</td>
</tr>
<tr>
<td>Is List of Values</td>
<td>Check this check box to add multiple values to be associated with the rule input. A table appears where you can add, edit, and delete values. You can also set a default value.</td>
</tr>
<tr>
<td>Accept Multiple Values</td>
<td>Check this check box if you want to provide more than one value at the time of audit. This is applicable only for the execution type rule input.</td>
</tr>
<tr>
<td>Min Value</td>
<td>Enter a minimum integer value for the rule input. This is applicable only for the integer data type.</td>
</tr>
<tr>
<td>Max Value</td>
<td>Enter a maximum integer value for the rule input. This is applicable only for the integer data type.</td>
</tr>
<tr>
<td>Default Value</td>
<td>Enter a default value for the rule input. The format of the value that you enter in this field depends on the data type that you choose in the Data Type field. For example, if you choose Integer as the data type, you can enter an integer value only.</td>
</tr>
<tr>
<td>Max Length</td>
<td>Enter the maximum length that is applicable for the rule input.</td>
</tr>
<tr>
<td>Val RegExp</td>
<td>Enter a valid regular expression that will be used for execution or fix.</td>
</tr>
<tr>
<td><strong>Conditions and Actions</strong></td>
<td>Click New to create conditions and actions for the new rule.</td>
</tr>
</tbody>
</table>

New Conditions and Actions—Conditions Details Tab
# Chapter 31 Auditing Device Configurations to Ensure Compliance

## Creating Compliance Policies

### Condition Scope

Details

- **Condition Scope**—Select the scope of the conditions from one of the below:
  - Configuration—Checks the complete running configuration.
  - Device Command Outputs—Checks the output of show commands.
  - Device Properties—Checks against the device properties and not the running configuration.
  - Previously Matched Blocks—Runs the conditions against blocks that have been defined in previous conditions. To run the condition with this option, you must have checked Parse as Block option in one of the previous conditions. You cannot select this option for the first condition of a rule.

- **Device Property**—Select one of the following device properties:
  - Device Name
  - IP Address
  - OS Name
  - OS Version

*Note* This option is enabled only if you selected Device Properties in the Condition Scope drop-down list.

- **Show Commands**—Select the required show command that is applicable for the platform selected. You can also enter a show command against which the audit must be performed.

*Note* This option is enabled only if you selected Device Command Outputs in the Condition Scope drop-down list.

### Block Options

- **Parse as Blocks**
  - Checking this option enables you to run conditions on specific blocks (as defined in this section) in running configuration files. This option can be for show commands is enabled only if you selected Configuration in the Condition Scope option.

- **Block Start Expression**
  - This field is mandatory if Parse as Blocks option is enabled. This must be a regular expression. Rule inputs and Grep outputs can be used here.

- **Block End Expression**
  - This field is optional. By default, blocks end when the top-level or a sub-level command begins. If you prefer to break the block earlier, enter the value as a regular expression.

### Rule Pass Criteria

- **Check the option, as required. If you select:**
  - **All Sub Blocks**—The rule is marked a success only if all the blocks fulfill the specified condition.
  - **Any Sub Block**—The rule is marked a success even if one of the sub blocks fulfill the condition.
  - **Raise One Violation for Each Failing Instance**—If you check this option, the violation count specified in the Job view increases by as many number of violations as the condition encounters in each block.

### Condition Match Criteria

- **Operator**
  - Choose an option based on the value you will enter in the subsequent fields.

- **Operator Function**
  - Click Edit. The Select Operator Function page appears. Select a predefined function and enter the function parameters based on the predefined function that you have selected.

*Note* This field is available only if you selected the option, Execute a Function from the Operator field.

### Table 31-1 Configuration > Compliance > Policies > New Rule Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Condition Scope      | **Details**
|                      | - Condition Scope—Select the scope of the conditions from one of the below:
|                      |   - Configuration—Checks the complete running configuration.
|                      |   - Device Command Outputs—Checks the output of show commands.
|                      |   - Device Properties—Checks against the device properties and not the running configuration.
|                      |   - Previously Matched Blocks—Runs the conditions against blocks that have been defined in previous conditions. To run the condition with this option, you must have checked Parse as Block option in one of the previous conditions. You cannot select this option for the first condition of a rule.
|                      | - Device Property—Select one of the following device properties:
|                      |   - Device Name
|                      |   - IP Address
|                      |   - OS Name
|                      |   - OS Version
|                      | *Note* This option is enabled only if you selected Device Properties in the Condition Scope drop-down list.
|                      | - Show Commands—Select the required show command that is applicable for the platform selected. You can also enter a show command against which the audit must be performed.
|                      | *Note* This option is enabled only if you selected Device Command Outputs in the Condition Scope drop-down list.

- **Block Options**
  - **Parse as Blocks**
    - Checking this option enables you to run conditions on specific blocks (as defined in this section) in running configuration files. This option can be for show commands is enabled only if you selected Configuration in the Condition Scope option.

- **Block Start Expression**
  - This field is mandatory if Parse as Blocks option is enabled. This must be a regular expression. Rule inputs and Grep outputs can be used here.

- **Block End Expression**
  - This field is optional. By default, blocks end when the top-level or a sub-level command begins. If you prefer to break the block earlier, enter the value as a regular expression.

- **Rule Pass Criteria**
  - Check the option, as required. If you select:
    - **All Sub Blocks**—The rule is marked a success only if all the blocks fulfill the specified condition.
    - **Any Sub Block**—The rule is marked a success even if one of the sub blocks fulfill the condition.
    - **Raise One Violation for Each Failing Instance**—If you check this option, the violation count specified in the Job view increases by as many number of violations as the condition encounters in each block.

- **Condition Match Criteria**
  - **Operator**
    - Choose an option based on the value you will enter in the subsequent fields.

  - **Operator Function**
    - Click Edit. The Select Operator Function page appears. Select a predefined function and enter the function parameters based on the predefined function that you have selected.

*Note* This field is available only if you selected the option, Execute a Function from the Operator field.
Creating Compliance Policies

Chapter 31  Auditing Device Configurations to Ensure Compliance

### Table 31-1  Configuration > Compliance > Policies > New Rule Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>The value must be a regular expression. Rule inputs and Grep outputs can be used here. This variable can be grepped for use in the subsequent conditions. It follows the convention of condition <code>&lt;number.value number&gt;</code> such as, <code>&lt;2.1&gt; &lt;2.2&gt;...</code> This numerical identifier can be used from the next condition as input parameter for Operator selected in the previous field.</td>
</tr>
<tr>
<td>Rule Pass Criteria</td>
<td>Check the option, as required. If you select:</td>
</tr>
<tr>
<td></td>
<td>• All Sub Blocks—The rule is marked a success only if all the blocks fulfill the specified condition.</td>
</tr>
<tr>
<td></td>
<td>• Any Sub Block—The rule is marked a success even if one of the sub blocks fulfill the condition.</td>
</tr>
<tr>
<td></td>
<td>• Raise One Violation for Each Failing Instance—If you check this option, the violation count specified in the Job view increases by as many number of violations as the condition encounters in each block.</td>
</tr>
</tbody>
</table>

**New Conditions and Actions—Action Details Tab**

<table>
<thead>
<tr>
<th>Select Action</th>
<th>Select one of the following actions that Compliance Audit must perform upon detecting a violation:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Continue—If the condition is met or not met, the rule continues to run based on the condition number specified in the field. If a condition number is not specified, the rule skips to the next immediate condition.</td>
</tr>
<tr>
<td></td>
<td>• Does Not Raise a Violation—Does not raise a violation; stops further execution of rule.</td>
</tr>
<tr>
<td></td>
<td>• Raise a Violation—Raises a violation and stops further execution of rule.</td>
</tr>
<tr>
<td></td>
<td>• Raise a Violation and Continue—Raises a violation and continues execution of rule.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Condition Number</th>
<th>Specify the condition number to which the rule must continue with in case the condition is met or is not met. You cannot specify a condition number that is lesser than or equal to the current condition number. This field is available only if you selected the option Continue from the Select Action field. If the Condition Number field is blank, the next available condition is used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violation Severity</td>
<td>Specify a severity that Compliance Audit must flag if a violation is detected. This field is available only if you selected the option, Raise a Violation from the Select Action field.</td>
</tr>
<tr>
<td>Violation Message</td>
<td>Select one of the following message type:</td>
</tr>
<tr>
<td>Type</td>
<td>• Default Violation Message—Select this option if you determine a violation as not fixable (or requiring manual intervention).</td>
</tr>
<tr>
<td></td>
<td>• User defined Violation Message—Select this option to enter a comment and provide a CLI fix to fix a violation.</td>
</tr>
<tr>
<td></td>
<td>This field is available only if you selected the option, Raise a Violation from the Select Action field.</td>
</tr>
</tbody>
</table>

| Violation Message   | **Note** This field is available only if you selected User defined Violation Message in the Violation Message Type field.                                                                                 |
|                    | Enter a violation message that will be displayed in the Job View window. Rule inputs can be used here.                                                                                                       |
Creating Compliance Policies

Importing and Exporting Policies

Step 1 Choose Configuration > Compliance > Policies.
Step 2 From the left navigation pane, select the policy which needs to be imported or exported.
Step 3 To export policy—Hover the mouse over the required policy and click Export Policy as XML and click Save.
Step 4 To import policy—In the left navigation pane, hover the mouse over the Import Policy as XML icon and click. Click Choose Files and click Import.

Related Topics
- Compliance Auditing Prerequisites
- Creating Compliance Policies
- Configuration > Compliance > Policies

Sample Compliance Policy Rules

The following sections contain sample compliance policies and the rules contained in each of them.

DNS Servers Configured on Device

This compliance policy checks if either IP name-server 1.2.3.4 or IP name-server 2.3.4.5 is configured on the device, and raises a violation if neither of them are configured.

You must enter the following settings in the appropriate fields of the Configuration > Compliance > Policies > New Rule form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition Scope Details</td>
<td>Configuration</td>
</tr>
<tr>
<td>Block Options (optional)</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 31  Auditing Device Configurations to Ensure Compliance

Creating Compliance Policies

NTP Server Redundancy

This compliance policy checks if the command `ntp server` appears at least twice on the device.
You must enter the following settings in the appropriate fields of the Configuration > Compliance > Policies> New Rule form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Matches the expression</td>
</tr>
<tr>
<td>Value</td>
<td>`ip name-server (1.2.3.4</td>
</tr>
<tr>
<td>Match Action</td>
<td>Do not raise a violation and exit this rule</td>
</tr>
<tr>
<td>Does Not Match Action</td>
<td>Raise a violation and exit this rule</td>
</tr>
<tr>
<td>Violation Text</td>
<td>DNS Server must be configured as either 1.2.3.4 or 2.3.4.5.</td>
</tr>
</tbody>
</table>

Community Strings

This compliance policy checks if either `snmp-server community public` or `snmp-server community private` is configured on the device. If configured, Prime Infrastructure raises a violation.
You must enter the following settings in the appropriate fields of the Configuration > Compliance > Policies> New Rule form.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition Scope Details</td>
<td>Configuration</td>
</tr>
<tr>
<td>Operator</td>
<td>Matches the expression</td>
</tr>
<tr>
<td>Value</td>
<td><code>{ntp server.*\n}{2,}</code></td>
</tr>
<tr>
<td>Match Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Does Not Match Action</td>
<td>Raise a violation and exit this rule</td>
</tr>
<tr>
<td>Violation Text</td>
<td>Community string &lt;1.1&gt; configured.</td>
</tr>
</tbody>
</table>

In the violation text, `<1.1>` is replaced with the actual community string configured on the device at runtime. In this example, `<1.1>` indicates the first captured group in the current condition.

IOS Software Version

This compliance policy checks if Cisco IOS software version 15.0(2)SE7 is installed on a device.
You must enter the following settings in the appropriate fields of the Configuration > Compliance > Policies > New Rule forms.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition Scope Details</td>
<td>Device Command Outputs</td>
</tr>
<tr>
<td>Show Commands</td>
<td>show version</td>
</tr>
<tr>
<td>Operator</td>
<td>contains the string</td>
</tr>
<tr>
<td>Value</td>
<td>15.0(2)SE7</td>
</tr>
<tr>
<td>Match Action</td>
<td>Continue</td>
</tr>
<tr>
<td>Does Not Match Action</td>
<td>Raise a Violation</td>
</tr>
<tr>
<td>Violation Text</td>
<td>Output of show version must contain the string ‘15.1(1)SY2’.</td>
</tr>
</tbody>
</table>

### Policy Group Details

Table 31-2 describes the policy group details.

**Table 31-2  List of Policy Groups**

<table>
<thead>
<tr>
<th>Policy Group Name</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA Services</td>
<td>• AAA</td>
</tr>
<tr>
<td></td>
<td>• AAA Accounting—Connections</td>
</tr>
<tr>
<td></td>
<td>• AAA Accounting—Exec</td>
</tr>
<tr>
<td></td>
<td>• AAA Accounting—Network</td>
</tr>
<tr>
<td></td>
<td>• AAA Accounting—System</td>
</tr>
<tr>
<td></td>
<td>• AAA Authentication—Enable</td>
</tr>
<tr>
<td></td>
<td>• AAA Authentication—Login</td>
</tr>
<tr>
<td></td>
<td>• AAA Authorization—Configuration</td>
</tr>
<tr>
<td></td>
<td>• AAA Authorization—Exec</td>
</tr>
<tr>
<td></td>
<td>• AAA Authorization—Network</td>
</tr>
<tr>
<td>Audit and Management</td>
<td>• Banners</td>
</tr>
<tr>
<td></td>
<td>• Console Access</td>
</tr>
<tr>
<td></td>
<td>• DHCP</td>
</tr>
<tr>
<td></td>
<td>• Domain Name</td>
</tr>
<tr>
<td></td>
<td>• Host Name</td>
</tr>
<tr>
<td></td>
<td>• Logging and Syslog</td>
</tr>
<tr>
<td></td>
<td>• Terminal Access</td>
</tr>
<tr>
<td></td>
<td>• User Passwords</td>
</tr>
</tbody>
</table>
Table 31-2 List of Policy Groups (continued)

<table>
<thead>
<tr>
<th>Policy Group Name</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Configuration</td>
<td>• ACLs</td>
</tr>
<tr>
<td></td>
<td>• CDP</td>
</tr>
<tr>
<td></td>
<td>• Clock</td>
</tr>
<tr>
<td></td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td>• NTP Configuration</td>
</tr>
<tr>
<td></td>
<td>• Traceroute</td>
</tr>
<tr>
<td>Network Access Services</td>
<td>• Loopback Interfaces</td>
</tr>
<tr>
<td></td>
<td>• Remote Commands</td>
</tr>
<tr>
<td>Network Protocols</td>
<td>• Control Plane Policing</td>
</tr>
<tr>
<td></td>
<td>• Hot Standby Router Protocol (HSRP)</td>
</tr>
<tr>
<td></td>
<td>• ICMP</td>
</tr>
<tr>
<td></td>
<td>• Miscellaneous Services</td>
</tr>
<tr>
<td></td>
<td>• Routing and Forwarding</td>
</tr>
<tr>
<td></td>
<td>• TCP Parameters</td>
</tr>
<tr>
<td>Others</td>
<td>• Device Version Checks</td>
</tr>
<tr>
<td>Routing Protocols</td>
<td>• BGP</td>
</tr>
<tr>
<td></td>
<td>• EIGRP</td>
</tr>
<tr>
<td></td>
<td>• OSPF</td>
</tr>
<tr>
<td></td>
<td>• RIP</td>
</tr>
<tr>
<td>Security</td>
<td>• ACL on Interfaces</td>
</tr>
<tr>
<td></td>
<td>• Distributed DoS Attacks</td>
</tr>
<tr>
<td></td>
<td>• Firewall Traffic Rules</td>
</tr>
<tr>
<td></td>
<td>• Land Attack</td>
</tr>
<tr>
<td></td>
<td>• Martian Traffic</td>
</tr>
<tr>
<td></td>
<td>• Null (Black Hole) Routing</td>
</tr>
<tr>
<td></td>
<td>• Risky Traffic</td>
</tr>
<tr>
<td></td>
<td>• SMURF Attack</td>
</tr>
<tr>
<td></td>
<td>• Traffic Rules</td>
</tr>
</tbody>
</table>
### Table 31-2  List of Policy Groups  (continued)

<table>
<thead>
<tr>
<th>Policy Group Name</th>
<th>Policies</th>
</tr>
</thead>
</table>
| Switching         | • DHCP Snooping  
|                   | • Dynamic Trunking Protocol  
|                   | • IEEE 802.1x Port-Based Authentication  
|                   | • IEEE 802.3 Flow Control  
|                   | • IP Phone + Host Ports  
|                   | • IP Phone Ports  
|                   | • Management VLAN  
|                   | • Port Security  
|                   | • Spanning Tree Protocol (STP)  
|                   | • Unidirectional Link Detection (UDLD)  
|                   | • Unused Ports  
|                   | • VLAN 1  |
| Compliance Policies | All user-defined policies are listed under this policy group. Eight example policies are available.  
|                   | • All interfaces should restrict traffic  
|                   | • Block incoming telnets using un-authorized protocols  
|                   | • Check DNS Servers are configured  
|                   | • NTP Server redundancy  
|                   | • SMU verification on ASR  
|                   | • OSPF MD5 Check  
|                   | • SNMP prohibit well known community strings  
|                   | • Trap Destination  |
| Wireless Policies | • CDP Status  
|                   | • Check Authentication Servers  
|                   | • Check IDS Status  
|                   | • NTP Server should be configured  
|                   | • SNMP Status  
|                   | • Syslog Status  
|                   | • Telnet Status  
|                   | • WLAN Security Status  
|                   | • Web Mode Status  |

### Grouping Policies into Compliance Profiles

After you have created compliance policies, you can create a policy profile that contains a set of policies.
Running Compliance Profiles Against Devices

After you create a compliance profile, you choose the devices on which to run it. Prime Infrastructure creates a job with the name of the compliance profile.

Step 1  After you create a compliance profile, click the Run Compliance Audit icon.
Step 2  Select the devices which you wish to audit. Click Next.
Step 3  In the Schedule Audit page, enter the schedule details. In the Choose Configuration option, select one of the following:
  • Use Latest Archived Configuration—If you choose this option, Prime Infrastructure uses the latest backup configuration in the archive. If the backup configuration is not available, the device is not audited and is marked against non-audited devices.
  • Use Current Device Configuration—Prime Infrastructure polls for the latest configuration from the device and then performs the audit. If a Show command is used in the compliance policy, the output of the Show command is taken from the current device configuration.
Step 4  Click Next.
Step 5  Select Now to schedule the audit job immediately or select Date and enter a date and time to schedule it later.
   Select the appropriate radio button to repeat the audit job at regular intervals.
Step 6  Click Finish. An audit job is scheduled. To view the status of the audit job, choose Configuration > Compliance > Jobs.
Related Topics
- Creating Compliance Policies
- Grouping Policies into Compliance Profiles
- Viewing Compliance Audit Results
- Viewing Violation Summary Details

Viewing Compliance Audit Results

Choose Configuration > Compliance > Jobs to view the status of scheduled jobs and view any violations. There might be several different compliance policies running on a single device.

After a job is created, you can set the following preferences for the job:
- Pause Series—Can be applied only on jobs that are scheduled in the future. You cannot suspend a job that is running.
- Resume Series—Can be applied only on jobs that have been suspended.
- Edit Schedule—Reschedule a job that has been scheduled for a different time.

The Last Run Result column indicates the result of the compliance job as described in Table 31-3.

<table>
<thead>
<tr>
<th>Last Run Result Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure</td>
<td>One or more devices audited have a violation in the policies specified in the profile.</td>
</tr>
<tr>
<td>Partial Success</td>
<td>The compliance job contains a mix of both audited and non-audited devices, and the compliance status of audited devices is successful.</td>
</tr>
<tr>
<td>Success</td>
<td>All devices audited conform to the policies specified in the profile.</td>
</tr>
</tbody>
</table>

To view the details of a job, click the hyperlinked result displayed against each job.

Related Topics
- Fixing Compliance Violations on Devices
- Viewing Violation Summary Details

Configuration > Compliance > Jobs

Table 31-4 displays the information about the audited/non-audited devices, rules that you selected for the compliance audit, compliance state, violation count, instance count, highest severity and ignore count.
Fixing Compliance Violations on Devices

Prime Infrastructure allows you to fix any compliance violations that appear on devices.

### Step 1
Choose **Configuration > Compliance > Jobs**, then click the **Audit Jobs** tab to view the status of the jobs.

### Step 2
Click **Failure** under the Last Run Result column for any job in which compliance violations were found. Prime Infrastructure displays the status of all policies that were run as part of the compliance audit.

The Ignore Count column indicates the number of devices for which the specified policy is not applicable and therefore, was not validated against.

### Step 3
Click **Next** to view the devices on which the compliance violation appears.

### Step 4
Click the down arrow to expand the device name to view the policy for which there is a violation. When a device’s configuration contains a compliance violation, a check box appears when:

- There is an available CLI fix for the device.
- There is no job currently running to fix the violation.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Audited/Non-Audited Devices | This displays the number of audited and non-audited devices. For more details on devices, click the hyperlinked count of audited and non-audited devices. The device name and audit status are displayed when you click the hyperlinked count of audited devices. Non-audited devices include the count of the following.  
  - The devices that were within the scope of the user while scheduling the job, but has since changed. At the time job ran, these devices were not within the scope of the user.  
  - The devices that were down or were not reachable when the job ran.  
  - CPT device not in IOS mode. These devices are not audited because they do not contain running configuration, which is required for Compliance Manager.  
  - Third Party Devices.  
  - Device not in sync with Compliance server—that is, the device element type is not available in the Compliance server. |
| Selected Rules         | Number of rules selected in a policy at the time the policy profile was created. This may be subset of the total number of rules defined for the policy.                                                        |
| Compliance State       | Displays Pass or Fail. All rules in policy for all devices must confirm for the state to display Pass.                                                                                                      |
| Violation Count        | This lists the number of distinct violations (for a particular policy, for the number of devices) that were observed in each job. For example, if a particular policy is violated in 100 devices, the violation count is only 1. |
| Instance Count         | Summation of the violation count for all the device. For example, if a particular policy is violated in 100 devices, the instance count is 100.                                                             |
| Highest Severity       | The highest severity of the various rules comprising the policy. The highest (as decided at the time of creating rules) is shown. This overrides the lower severity items.                             |
| Ignore Count           | This is the count of rules ignored due to devices falling outside the scope of platforms defined against the rule.                                                                                           |
Step 5 Select the box next to the policy for which you have defined and want to apply a fix, then click Next.

Step 6 Preview the fix commands that were previously defined in the policy, then click Next.

Step 7 Select the schedule for applying the configuration changes to the device, then click Schedule Fix Job.

Related Topics
- Creating Compliance Policies
- Grouping Policies into Compliance Profiles
- Viewing Compliance Audit Results
- Viewing Violation Summary Details

Viewing Violation Summary Details

You can run a report to display the violation summarized details for all the audit jobs that failed. To generate the report, follow these steps:

Step 1 Choose Configuration > Compliance > Jobs, then click the Violation Summary tab.

Step 2 The report displays the summarized details of the job failure.

Step 3 You can download the reports in PDF and CSV formats.

Viewing Device Security Vulnerabilities

You can run a report to determine if any devices in your network have security vulnerabilities as defined by the Cisco Product Security Incident Response Team (PSIRT). You can also view documentation about the specific vulnerability that describes the impact of a vulnerability and any potential steps needed to protect your environment.

Step 1 Choose Reports > PSIRT and EoX.

Step 2 You need to sync the devices prior to scheduling the job. Choose Configuration > Network Devices > Select all Devices. Click Sync.

Step 3 Click Schedule Job. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.

Step 4 Click View Job Details to view the current status of the PSIRT report. On completion of the job, you can see COMPLETED_WITH_SUCCESS as the operation status with the execution log details.

Step 5 Click the Device PSIRT tab to view PSIRT information.

Step 6 In the PSIRT Title column, click the hyperlink to view the full description of the security vulnerability.

Step 7 You can download the PSIRT report in PDF and CSV formats.
Viewing End-of-Life Reports

You can run a report to determine if any Cisco device hardware or software in your network have reached its end of life (EOX). This can help you determine product upgrade and substitution options.

**Step 1** Choose **Reports > PSIRT and EoX**.

**Step 2** Click **Schedule Job**. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.

**Step 3** After the job completes, click one of the following EOX tabs to view the report information specific to that tab:

- Device Hardware EOX
- Device Software EOX

Viewing Field Notices for Devices

You can run a report to determine if any Cisco devices that are managed and have completed a full inventory collection have any field notices. Field Notices are notifications that are published for significant issues, other than security vulnerability-related issues, that directly involve Cisco products and typically require an upgrade, workaround, or other customer action.

**Step 1** Choose **Reports > PSIRT and EoX**.

**Step 2** Click **Schedule Job**. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.

**Step 3** Click the **Field Notice** tab to view field notice information.

**Step 4** Click on the hyperlink in the Field Notice Name column to view more information on cisco.com.
Configuring Plug and Play

Prime Infrastructure helps automate the deployment of new devices on the network by obtaining and applying the necessary software image and configuration on a new network device. Using features such as Cisco Network Services (CNS) call-home, APIC-EM (Application Policy Infrastructure Controller) call-home and Cisco IOS auto-install (which uses DHCP and TFTP), Prime Infrastructure reduces the time a new device takes to join the network and become functional.

The Plug and Play feature of Prime Infrastructure uses the templates defined in Configuration > Features and Technologies that you can reuse and apply to new devices. You can streamline new device deployment by creating bootstrap templates, which define the necessary initial configurations to enable the device to communicate with Prime Infrastructure. You can specify (and predeploy) software images and configurations that will be added to the devices in the future. See Using Templates to Configure Devices to know more on template creation.

Related Topics
- Prerequisites for Delivering Plug and Play Profiles
- Plug and Play Workflow

Prerequisites for Delivering Plug and Play Profiles

Based on the method that you select to deliver the Plug and Play profile to new devices, you must make sure that you have completed the necessary prerequisites.

- Configure DHCP with the appropriate settings in the network as described in Sample DHCP Server Settings.
- You must have an existing network connection (distribution/core) available in the branch or campus to where the new device is connecting.
- The branch must have direct connectivity to the Prime Infrastructure server, or you must use the Plug and Play external server to connect to Prime Infrastructure.
- Ensure TFTP is enabled on the Prime Infrastructure server by choosing Administration > Settings > System Settings > Server, then clicking Enable under TFTP. TFTP is enabled by default. This is an optional requirement for APIC-EM mode.
Plug and Play Workflow

Prime Infrastructure allows you to perform an initial provisioning of a software image and configuration on a new device. To automate the deployment of a new device on your network, follow this workflow:

1. Specify which of the following servers Prime Infrastructure uses for Plug and Play. If you do not specify the server, CNS gateway will be enabled by default.
   - CNS gateway—You use the CNS gateway that is bundled with Prime Infrastructure by default, or use an external CNS gateway.
   - APIC-EM—You can specify that Prime Infrastructure uses APIC-EM for Plug and Play. See Integrating APIC-EM with Prime Infrastructure for information about setting up APIC-EM.

2. Create a Plug and Play profile for your devices. The profiles are categorized as Routers, Switches, Wireless AP and Nexus Profiles. See Plug and Play Profiles.

3. Power on the device.

4. Apply a bootstrap configuration to the device. The bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the Prime Infrastructure gateway (CNS or APIC-EM). See Bootstrap Configuration.
   
   In the case of Wireless AP profiles, the Primary, Secondary and Tertiary WLC details are required. See Creating Plug and Play Profiles for Wireless AP.

   In the case of Nexus devices, the Plug and Play workflow differs as these devices do not support bootstrap configuration. See Creating Plug and Play Profiles for Nexus Devices for more details.

After you apply the initial configuration:

1. The device communicates with the Prime Infrastructure server.

2. Based on the Device Plug and Play ID / serial number, Prime Infrastructure verifies if this matches with the device ID in any of the Plug and Play preprovisioning definitions.

3. If there is a match, Prime Infrastructure applies the software image and the configuration specified in the matched Plug and Play profile on the device.
   
   If there is no match for the device ID, Prime Infrastructure matches the device type with any of the existing type-based Plug and Play preprovisioning definitions.

4. The device is added to its inventory and is managed by Prime Infrastructure.

5. Once the device is added and managed in the inventory, Prime Infrastructure applies the post Plug and Play configurations, if specified in the Plug and Play profile, on the device.
After the bootstrap configuration is applied to the device, the installer connects the device to a WAN at the remote site. The device connects to the Plug and Play gateway using its serial number, and downloads the full configuration and (optional) Cisco IOS image (see Figure 32-1).

**Figure 32-1   Plug and Play Branch Deployment**

Choose Configuration > Plug and Play > Dashboard and select the Home tab to view the dashboard of the Plug and Play application.
### Viewing Plug and Play Dashboard

1. Click **About** to know about Plug and Play feature. See Configuring Plug and Play.
2. Click **Monitoring** to view the details of devices in a map view. See Integrating Map View.
3. Click **Errors / Progress / Success** to navigate to **Device Status** page. The details will be filtered and displayed accordingly.
4. Click to navigate to **Device Status** page to monitor the devices and its status.
5. Click to navigate to **Bootstrap** page to create bootstrap templates for profiles.
6. Click to navigate to **Administration > Servers > APIC-EM Controller** page.
7. Click to navigate to **Plug and Play Profiles** page to create profile for a device type.
8. Click to navigate to **Profile Activation** page to activate by providing values specific to device/type.
9. Click to navigate to **Device Status** page.
10. Click to navigate to **Map View** page to view the devices and their site locations.
11. Click to navigate to **Plug and Play Profiles** page.
12. Click to navigate to **Administration > Dashboard > Jobs Dashboard** page to view the job status.

### Related Topics
- Integrating APIC-EM with Prime Infrastructure
- Integrating Map View
- Plug and Play Profiles
- Activating Device Profiles
- Bootstrap Configuration
- Verifying Device Status
APIC-EM and Plug and Play

Prime Infrastructure supports APIC-EM GA Release 1.0.0.x. You can specify to have Prime Infrastructure use the APIC-EM for Plug and Play. You must preconfigure a profile which determines what is deployed on the devices (configurations, images, etc.). When the device calls home, based on the device’s serial number, the profile is matched and the device is provisioned with the same pre-configured image and configuration from Prime Infrastructure using APIC-EM’s Plug and Play.

With APIC-EM Plug and Play integration, devices can be provisioned with http/https. If applicable, when the profile is created, you can also choose to install PKI (Public Key Infrastructure) and SUDI (Secure Unique Device Identifier) certificates on the device to use PKI and SUDI based authentication.

**Note**
Prime Infrastructure supports only APIC-EM for Wireless AP profiles.

**Related Topics**
- Integrating APIC-EM with Prime Infrastructure
- Plug and Play Workflow

Integrating APIC-EM with Prime Infrastructure

Prime Infrastructure communicates with APIC-EM via HTTPs and REST API’s exposed by APIC-EM.

**Note**
Prime Infrastructure requires a dedicated APIC-EM server. Hence you must not integrate the APIC-EM server with more than one Prime Infrastructure server to prevent data corruption and out of sync condition.

To integrate APIC-EM controller to Prime Infrastructure, follow these steps:

**Step 1** Choose **Configuration > Plug and Play > Dashboard**.
**Step 2** In the **Home** tab, click on **Server** to view the **Administration > Servers > APIC-EM Controller** page.
**Step 3** Click **Add**.
**Step 4** Enter the APIC-EM controller IPv4 address.
**Step 5** Enter the HTTPS port number to connect with APIC-EM.
**Step 6** Enter your user name.
**Step 7** Enter your password and confirm it.

The polling interval is not editable. The APIC-EM controller is polled periodically (every 5 minutes) to check the status of its connection / integration with Prime Infrastructure.

After the APIC-EM controller is added to Prime Infrastructure, you can view the reachability status of the APIC controller in same page. You can select a specific APIC-EM controller to view the history of the connection polling status. Make sure the APIC-EM connection is successful before using the service.

To navigate to **Configuration > Plug and Play > Dashboard**, click the link **Please Click here to create Plug and Play Profiles**.
Chapter 32  Configuring Plug and Play

Plug and Play Profiles

The global option in Administration > Servers > APIC-EM Controller > Global PnP/ZTD Settings is automatically set to APIC-EM when you add a valid APIC-EM controller into Prime Infrastructure.

**Related Topics**

- Plug and Play Profiles
- Bootstrap Configuration
- Viewing Plug and Play Dashboard

**APIC-EM Site Sync**

Prime Infrastructure can integrate and synchronize its inventory with APIC-EM. You need to have a dedicated instance of Prime Infrastructure that integrates with APIC-EM. The dedicated Prime Infrastructure instance can be used for monitoring the network only, not for provisioning.

From the dedicated instance of Prime Infrastructure, specify the APIC-EM instance from the Administration > Servers > APIC-EM Controller page. This Prime Infrastructure instance periodically syncs the sites, devices, device and location groups, WAN interface port groups, and endpoint associations with the APIC-EM instance. Prime Infrastructure collects inventory and other monitoring information for the synced devices and creates a new folder under All Devices > Location and adds the devices to the corresponding sites. Prime Infrastructure monitors the devices by collecting assurance and syslog information.

By default, Prime Infrastructure runs an APIC-EM integration sync job every six hours. If you remove sites and devices from APIC-EM, they are also deleted from Prime Infrastructure. If devices are added or updated in APIC-EM, Prime Infrastructure will also add and update them.

**Plug and Play Profiles**

Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles. The detailed summary of the list of plug and play profiles are displayed.

Prime Infrastructure helps you create a Plug and Play Profile that allows any newly connected device to “call home” to the Prime Infrastructure server so that the device can be discovered, added to the inventory, and configured. This profile, also known as a Bootstrap Profile, places credentials on the device, eliminating the need to “console” into every device to setup before the device can be managed by Prime Infrastructure.

You can create any of the following Plug and Play profiles under the specific folders:

- Router profiles - See Creating Plug and Play Profiles for Routers and Switches
- Switch profiles - See Creating Plug and Play Profiles for Routers and Switches
- Wireless AP profiles - See Creating Plug and Play Profiles for Wireless AP
- Nexus profiles - See Creating Plug and Play Profiles for Nexus Devices

Depending on the type, you can create Plug and Play profiles that contain:

- Software images only.
- Configurations only.
- Both software images and configurations.
- PKI certificates and SUDI certificates (For APIC-EM only.)
- Primary and Secondary Controllers, AP and Flexconnect groups (For Wireless AP only.)

The profile can include additional post Plug and Play configurations (optional), that can be applied on the device only after the device is managed by Prime Infrastructure.

**Note**
You cannot create a profile under the root Plug and Play Profiles folder. Depending on the profile-type, you can create profiles only under the specific folders - Nexus Profiles, Switch Profiles, Router Profiles and Wireless AP Profiles.

**Related Topics**
- Prerequisites for Connecting a Nexus Device in the Network
- Activating Device Profiles
- Viewing Plug and Play Dashboard
- Bootstrap Configuration
- Verifying Device Status
- Deleting Plug and Play Profiles

### Creating Plug and Play Profiles for Routers and Switches

A Plug and Play profile must have *at least one* of the following:
- A bootstrap configuration—Prime Infrastructure provides a standard bootstrap configuration, or you can create your own. See Bootstrap Configuration.
- Software image—See Managing Software Images.
- Configuration CLI template (PnP and Post PnP configuration)—See CLI Templates.

**Step 1**
Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

**Step 2**
Select the required profile (Router Profiles or Switch Profiles) from the left navigation pane, then click Add to view the details in Profile Summary tab.

**Step 3**
Provide the required information in the Profile Basic section.
- If you select Router or Switch from the Device Type drop-down list, then you will be required to select the required credential profile from the Credential Profile drop-down list to associate the credentials common to the device. See Using Credential Profiles.

**Step 4**
(Optional) If you have selected APIC-EM for Plug and Play, in the Profile Detail section, check the Enable Terminal Server check box to provision devices with terminal server IP and port.

**Step 5**
(Optional) If you have selected APIC-EM for Plug and Play, in the Profile Detail section, check the Enable PKI check box to provision devices with PKI certificates. PKI certificates are installed on the device after the Image provision and configuration are complete. See Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E for more information.

The Enable Terminal Server and Enable PKI options are available for users who have selected APIC-EM as the Plug and Play server. You cannot select this option if you selected CNS as the Plug and Play server.

If the Enable PKI check box is unchecked, the device is not provisioned with PKI certificates.
Chapter 32  Configuring Plug and Play

Note

Enable PKI check box will be disabled for Switch Profiles.

Step 6  (Optional) If you selected APIC-EM for Plug and Play, in the Profile Detail section, check the Enable SUDI check box to provision devices with SUDI certificates. By enabling this option, you can specify that the APIC-EM controller must validate the SUDI certificate to authenticate the device.

Step 7  From the Bootstrap Template drop-down list, select the bootstrap templates. You can also create a customized bootstrap template which will be saved in PnP Bootstrap Templates (User Defined). See Bootstrap Configuration.

Step 8  (Optional) From the Software Image drop-down list, select the required software images. This step is required only if you want to provision the device with images. See Importing Software Images for Plug and Play Profiles.

The Image Location text box is disabled if you selected APIC-EM for Plug and Play.

Step 9  (Optional) From the Configuration Template drop-down list, select a previously created configuration template.

Step 10  (Optional) From the Post PnP Configuration Template drop-down list, select the required configuration template. This configuration is applied on the device once it is managed by Prime Infrastructure.

Step 11  Click Save as New Plug and Play Profile.

Step 12  The profile is created and the details in Profile Summary tab is displayed. You can edit the details and click Save to save the details in the same profile and click Save as New to create a new profile.

Step 13  Click Profile Instances tab.

Step 14  Click Add to add details for the devices for which you want to pre-provision the Plug and Play Profile. See Adding Device Profiles into Router and Switches Plug and Play Profiles.

Related Topics

- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Importing Device Profiles into Plug and Play Profiles
- Activating Device Profiles
- Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E
- Bootstrap Configuration

Importing Software Images for Plug and Play Profiles

You can import a software image to include it as part of a Plug and Play profile.

Step 1  Choose Inventory > Device Management > Software Images.

Step 2  Click Import, then specify the source from which the software image is to be imported.

Step 3  Specify the collection options and when to import the image file. You can run the job immediately or schedule it to run at a later time.

The image import job will run only once.

Step 4  Click Submit.
Step 5  To view the details of image management job, choose Administration > Dashboards > Job Dashboard.

Creating Plug and Play Profiles for Wireless AP

You can create a plug and play profile for a wireless AP to provision thousands of devices at a time.

Step 1  Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

Step 2  Select Wireless AP Profiles from the left navigation pane and click Add to view the details in the Profile Summary tab.

Step 3  Provide the required information in the Profile Basic section.

In the Device Type field, Autonomous AP is auto-populated and is non-editable. It is mandatory to provide the PID value for Wireless AP profiles.

Step 4  Provide the required information in the Profile Detail section.

Step 5  Click Save as New Plug and Play Profile.

Step 6  The profile is created and the details in Profile Summary tab is displayed. You can edit the details and click Save to save the details in the same profile and click Save as New to create a new profile.

Step 7  Click Profile Instances tab.

Step 8  Click Add to add details for the devices for which you want to pre-provision the Plug and Play Profile. See Adding Device Profiles into Wireless AP Plug and Play Profiles.

Related Topics

- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Bootstrap Configuration
- Verifying Device Status

Prerequisites for Connecting a Nexus Device in the Network

The following prerequisites should be met before connecting the Nexus device to the network:

- A DHCP server to bootstrap the interface IP address, gateway address, script server (Cisco Prime Infrastructure 3.1) and script file (Plug and Play). See Configuring DHCP Server.
- A TFTP or HTTP server containing the configuration script used to automate the software image installation and configuration process. See Configuring HTTP Server.
- Cisco Prime Infrastructure 3.1 server with created Plug and Play Nexus profile containing the software images and configuration files. See Creating Plug and Play Profiles for Nexus Devices.
- The Nexus device version must be higher than 6.2(12) or later to manage all the Nexus features in Prime Infrastructure.
Configuring DHCP Server

The Nexus device sends out DHCP discover messages on all of the active interfaces (including the management interface) soliciting DHCP offers from the DHCP server or servers. The DHCP client on the Nexus device uses the device serial number or its MAC address in the client-identifier option to identify itself to the DHCP server. The DHCP server uses this identifier to send information, such as the IP address and script file name, back to the DHCP client.

The DHCP discover message also mandates the following options:

- Option 66 (TFTP server name) or Option 150 (TFTP server address)—The DHCP server relays the TFTP server name or TFTP server address to the DHCP client. The DHCP client uses this information to contact the TFTP server to obtain the script file.
- IP address
- Default Gateway
- Option 67 (Bootfile name)—The DHCP server relays the bootfile name to the DHCP client. The bootfile name includes the complete path to the bootfile on the TFTP server which is used by the DHCP client to download the script file.

Related Topics
- Configuring HTTP Server
- Creating Plug and Play Profiles for Nexus Devices
- Prerequisites for Connecting a Nexus Device in the Network
- Adding Device Profiles into Nexus Plug and Play Profiles

Configuring HTTP Server

Choose Administration > Settings > System Settings > General and select Server from the left navigation menu.

In the HTTP Forward section, select Enable to enable the device to contact the Plug and Play Gateway for downloading initial configuration and image. The default port is 80 but you can still change the port configuration on the device.

Note

Restart Prime Infrastructure for the changes to reflect.

Related Topics
- Configuring DHCP Server
- Creating Plug and Play Profiles for Nexus Devices
- Adding Device Profiles into Nexus Plug and Play Profiles
- Prerequisites for Connecting a Nexus Device in the Network

Creating Plug and Play Profiles for Nexus Devices

To create a Plug and Play profile for Nexus devices, follow these steps:

Step 1

Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.
Step 2  Select **Nexus Profiles** from the left navigation pane and click **Add** to view the details in the **Profile Summary** tab.

Step 3  Provide the required information in the Profile Basic section. Select the required credential profile from the **Credential Profile** drop-down list to associate the credentials common to the device. See **Using Credential Profiles**.

Step 4  From the **System Image** and **Kick Start Image** drop-down lists, select the required software images. See **Importing Software Images for Plug and Play Profiles**.

**Note** While downloading from Cisco.com, ensure that both system and kick start images have the same image version.

Step 5  From the **Configuration Template** drop-down list, select either the system-defined Nexus POAP Configuration Template or a previously created configuration template and make additional changes.

Step 6  Click **Save as New Plug and Play Profile**.

Step 7  The profile is created and the details in **Profile Summary** tab is displayed. You can edit the details and click **Save** to save the details in the same profile and click **Save as New** to create a new profile.

Step 8  Click **Profile Instances** tab.

Step 9  Click **Add** to add details for the devices for which you want to pre-provision the Plug and Play Profile. See **Adding Device Profiles into Nexus Plug and Play Profiles**.

**Related Topics**
- **Prerequisites for Connecting a Nexus Device in the Network**
- **Importing Software Images for Plug and Play Profiles**
- **Viewing Plug and Play Dashboard**
- **Adding Device Profiles into Nexus Plug and Play Profiles**

## Activating Device Profiles

You can pre-provision a device on any defined profile, and activate by providing values specific to device/type. To add devices in bulk, see **Importing Device Profiles into Plug and Play Profiles**.

You can perform either one of the following:
- Create a new plug and play profile and add device profiles to the created plug and play profile. See **Creating New Plug and Play Profiles and Adding Device Profiles**.
- Add device profiles to an existing plug and play profile. See **Adding Device Profiles to an Existing Plug and Play Profile**.

Alternatively, you can choose **Configuration > Plug and Play > Dashboard**, in the **Home** tab, click **PnP Profiles** to create a new Plug and Play profile. After creating the required Plug and Play profile, click **Add** in the **Profile Instances** tab to add device profiles.

**Related Topics**
- **Adding Device Profiles into Router and Switches Plug and Play Profiles**
- **Adding Device Profiles into Wireless AP Plug and Play Profiles**
Creating New Plug and Play Profiles and Adding Device Profiles

Step 1  Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Profile Activation.
Step 2  In the Select PnP Profile page, select Add device by creating new Profile.
Step 3  Select the type of profile you want to create from the Profile Type drop-down list.
Step 4  Enter the required information in the Profile Basic and Profile Detail sections. See Plug and Play Profiles for information on profile creation.
Step 5  (Optional) Enter the Terminal Server IP and Port if the Enable Terminal Server check box has been selected while creating a Plug and Play profile.
Step 6  Click the arrow icon in the right to navigate to the Plug and Play Profile page to add device profiles to the created plug and play profile.
Step 7  (Optional) If the Enable Terminal Server check box is selected, import the raw configuration on the device by:
   1. Import the zip files which contains multiple text files. Each text file will contain raw configuration that needs to be applied to the device. You can also import a single text file if required. The name of the text file should be DeviceSerialID.txt. For example if the device ID is FGLABCD443f, the text file containing the configuration details must be FGLABCD443f.txt.
   2. A job will be triggered for processing these files and uploading to APIC when the files are uploaded successfully.
   3. Verify the configuration has been successfully applied to the corresponding devices in that profiles by going to that particular profile in APIC.

Related Topics

- Adding Device Profiles to an Existing Plug and Play Profile
- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

Adding Device Profiles to an Existing Plug and Play Profile

Step 1  Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Profile Activation.
Step 2  In the Select PnP Profile page, select Add device to an existing profile.
Step 3  Select the required profile from the Select Profile drop-down list, for which you need to add device profiles. See Plug and Play Profiles for information on profile creation.
Step 4  The details of the profile you selected gets auto-populated and are non-editable.
Step 5  Click the arrow icon in the right to navigate to the **Plug and Play Profile** page to add device profiles to the created plug and play profile.

---

### Related Topics
- Creating New Plug and Play Profiles and Adding Device Profiles
- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

---

### Adding Device Profiles into Router and Switches Plug and Play Profiles

To add a device profile to the required Plug and Play profile, follow these steps:

---

**Step 1**  In the **Plug and Play Device Provisioning Profile** page, provide the required information.
- Select the site location to which the device will be mapped from the **Location** drop-down list. This detail will be displayed in the Map View.

**Note**  Before you add a device to a specific location, create a location group in Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups. See Using Location Groups.

**Step 2**  Click the arrow icon in the right to navigate to the **Bootstrap Selection** page.

**Step 3**  In the **Bootstrap Selection** page, the bootstrap template you selected in the profile creation phase will get auto-populated. You can edit the values as required.
- Plug and Play Gateway Location—By default, the Prime Infrastructure server acts as the Plug and Play gateway server. You can modify the server by providing the external Plug and Play gateway IP address.

Click **CLI** to view the CLI summary of the bootstrap configured.

**Step 4**  Click the arrow icon in the right to navigate to the next pages.

**Note**  If you had selected **Software Image** and **Configuration Template** in the profile creation phase, the **Software Image**, **Configuration** and **Post PnP Configuration** tabs will be displayed in the **Profile Activation** page.

**Step 5**  (Optional) In the **Software Image** page, provide the required information.

**Step 6**  (Optional) In the **Configuration** page, the configuration template you selected in the profile creation phase will be auto-populated. Provide the required information and navigate to the next page.

Click **CLI** to view the CLI summary.

**Step 7**  (Optional) In the **Post PnP Configuration** page, the configuration template you selected in the profile creation phase will be auto-populated. Provide the required information and navigate to the next page.

Click **CLI** to view the CLI summary.
**Activating Device Profiles**

**Step 8** In the **Management Credentials** page, provide the required information. These device parameters will be applied on the devices on provisioning.

**Note** If the device type is a router or switch, then in the **Management Credentials** page, the credential profile you selected in the profile creation phase will be auto-populated and the values cannot be edited.

**Step 9** In the **Profile Activation Summary** page, the device details with their configurations is displayed.

**Step 10** Click **Finish** to provision the device profile.

On successful provisioning, the device profile will be displayed in the **Profile Instances** page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the **Device Status** page.

After the device is provisioned successfully, the device is added to the Prime Infrastructure inventory so that the device can be managed. The device is added to the Prime Infrastructure inventory based on the management parameters provided in the Plug and Play Profile. After the device is added successfully to the inventory, additional post Plug and Play configurations (if applicable) are applied on the device. If there is a mismatch in credentials, the device is added to the inventory, but it will not have “Managed” status.

**Related Topics**
- Importing Device Profiles into Plug and Play Profiles
- Plug and Play Profiles
- Creating Plug and Play Profiles for Routers and Switches
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

**Importing Device Profiles into Plug and Play Profiles**

You can perform import and export operations on device profiles in bulk. Instead of adding devices and specifying their attributes one at a time, you can import a CSV file that includes all the devices and their attributes. By performing bulk import, you can update the existing profiles and add new profiles. To update more than one device profile at a time, you can perform bulk export.

**Step 1** Choose **Configuration > Plug and Play > Dashboard** and in the **Home** tab, click **PnP Profiles**.

**Step 2** Select the required Plug and Play profile from the left navigation menu. The details in **Profile Summary** tab is displayed.

**Step 3** Click **Profile Instances** tab.

**Step 4** Select the device profiles check-boxes you need to edit and click **Export**.

The CSV file with the device properties will be exported. You can add devices or edit the properties of the existing devices in the spreadsheet. Do not change the attribute names while editing the spreadsheet.

**Note** If you want to export a blank CSV file, click **Export** without selecting any device profiles. A blank csv file will be exported even if there are no device profiles in the **Profile Instances** page.
Step 5  Click **Import** and choose the CSV file in which you entered the device details. Click **Upload**.

The CSV file is uploaded and a link to **Administration > Dashboard > Jobs Dashboard** is displayed.

Step 6  In the **Jobs Dashboard** page, click **Import** from the left navigation menu to view the job status of the bulk imported file.

---

**Related Topics**
- Creating Plug and Play Profiles for Routers and Switches
- Adding Device Profiles into Wireless AP Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

**Deployment Based on Device Type**

If you are using a CNS gateway only for Plug and Play, to deploy a Plug and Play profile based on the device type, you do not have to associate the device ID with the deployment profile. Device type-based deployment is useful primarily for switches that use the same set of images and configurations. Matching profiles are identified by the device type (PID) of the incoming device that is specified in the profile during the design phase.

During device type-based deployment:

1. The device type is matched hierarchically: Prime Infrastructure searches for a profile with the same device type as that of the incoming device. If the profile does not match the device type, Prime Infrastructure searches for a profile that is defined for a higher level of the device type in the hierarchy.

   For example:
   - If the ‘switch_profile’ in Prime Infrastructure is defined for ‘Switches and Hubs’ and the incoming device is of type Switches and Hubs > Catalyst 2928 Series Switches > Catalyst 2928-24TC-C switch, and
   - If there is no profile defined specifically for this switch (Catalyst 2928-24TC-C or Catalyst 2928 Series Switches), then the ‘switch_profile’ is considered for deployment.

2. If Prime Infrastructure has multiple matching deployment profiles for a given device type, then Prime Infrastructure chooses the deployment profile that is created or has been recently updated.

**Adding Device Profiles into Wireless AP Plug and Play Profiles**

Prime Infrastructure supports only APIC-EM for Wireless AP profiles. You must preconfigure a plug and play profile which determines the primary, secondary and tertiary WLC details that is required to be provisioned on the devices. See **Creating Plug and Play Profiles for Wireless AP**.

When the AP (Access Point) is connected to a network, the AP contacts the DHCP of the network to know the APIC-EM details. The AP then contacts the APIC-EM and based on the device’s serial number and PID, the profile is matched. AP contacts WLC which then pushes the image and configurations to the device.

To add a device profile to the required Plug and Play profile, follow these steps:

Step 1  In the **Plug and Play Device Provisioning Profile** page, provide the required information.
Chapter 32  Configuring Plug and Play

Activating Device Profiles

- Select the site location to which the device will be mapped from the Location drop-down list. This detail will be displayed in the Map View.

**Note** Before you add a device to a specific location, create a location group in Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups. See Using Location Groups.

**Step 2** In the Profile Activation Summary page, the device details with their configurations is displayed.

**Step 3** Click Finish to provision the device profile.

On successful provisioning, the device profile will be displayed in the Profile Instances page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the Device Status page.

**Related Topics**
- Activating Device Profiles
- Plug and Play Profiles
- Creating Plug and Play Profiles for Wireless AP
- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Adding Device Profiles into Nexus Plug and Play Profiles

### Adding Device Profiles into Nexus Plug and Play Profiles

Before you begin, there is a set of prerequisites to be met. See Prerequisites for Connecting a Nexus Device in the Network.

When a Nexus device is connected to the network, it follows the below workflow:

1. Locates the configured DHCP server and establishes communication to get the IP Address, gateway, script server (Cisco Prime Infrastructure 3.1) and the script file (Nexus Plug and Play profile).
2. The device then communicates with the Cisco Prime Infrastructure and downloads the created Plug and Play profile for Nexus device. See Creating Plug and Play Profiles for Nexus Devices.
3. The device then obtains the IP address of a TFTP server or URL of an HTTP server from which it downloads the image and the necessary configuration files.

To add a device profile to the required Plug and Play profile, follow these steps:

**Step 1** In the Plug and Play Device Provisioning Profile page, provide the required information.

- Select the site location to which the device will be mapped from the Location drop-down list. This detail will be displayed in the Map View.

**Note** Before you add a device to a specific location, create a location group in Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups. See Using Location Groups.

**Step 2** Click the arrow icon in the right to navigate to the Image Selection page.
The selected system and kick start images are auto-populated and cannot be edited.

**Step 3** Click the arrow icon in the right to navigate to the **Configuration** page.

The configuration template you selected in the profile creation phase will be auto-populated. You should provide the Management Interface IP Address, Management Route IP Address and the other required information. This management IP address is configured to enable Cisco Prime Infrastructure to reach the Nexus device.

Click **CLI** to view the CLI summary.

**Step 4** Click the arrow icon in the right to navigate to the **Management Credentials** page.

For Nexus devices, it is mandatory to specify the **Management IP Address** so that the device can be managed. Provide the other required information and navigate to the next page. These device parameters will be applied on the devices on provisioning.

**Step 5** In the **Profile Activation Summary** page, the device details with their configurations is displayed.

**Step 6** Click **Finish** to provision the device profile.

On successful provisioning, the device profile will be displayed in the **Profile Instances** page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the **Device Status** page. The device is added to the Prime Infrastructure inventory so that the device can be managed.

Related Topics
- Viewing Plug and Play Dashboard
- Plug and Play Profiles
- Prerequisites for Connecting a Nexus Device in the Network
- Creating Plug and Play Profiles for Nexus Devices
- Adding Device Profiles into Router and Switches Plug and Play Profiles
- Adding Device Profiles into Wireless AP Plug and Play Profiles

**Supported Devices and Software Images for Plug and Play**

Table 32-1 lists the devices and corresponding software images supported for CNS gateway.

<table>
<thead>
<tr>
<th>Supported Devices for Plug and Play</th>
<th>Minimum Software Image Version Supported</th>
<th>Verified Image Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 2960, 2960S</td>
<td>Cisco IOS Release 12.2(55)SE and later</td>
<td>Cisco IOS Release 12.2(55)SE5 and later</td>
</tr>
<tr>
<td>Catalyst 2960C</td>
<td>Cisco IOS Release 12.2.55(EX) and later</td>
<td>Cisco IOS Release 12.2.55(EX3) and later</td>
</tr>
<tr>
<td>Catalyst 2960-SF</td>
<td>Cisco IOS Release 15.0(2)SE and later</td>
<td>Cisco IOS Release 15.0(2)SE and later</td>
</tr>
<tr>
<td>Catalyst 3560V2, 3750v2, 3560-X, 3750-X</td>
<td>Cisco IOS Release 12.2(55)SE and later</td>
<td>Cisco IOS Release 12.2(55)SE and later</td>
</tr>
</tbody>
</table>
Prerequisites for Deploying Bootstrap Configuration into a Device

To deploy bootstrap configuration into a device in a Prime Infrastructure Server:

- Enable Cipher in Admin mode of the server by entering the following command.
  
  $ ncs run pnp-ciphers enable
  
- Click Enable in the HTTP Forward section of the Administration > Settings > System Settings > Server Settings page.

- If you are going to use email to deliver either the bootstrap configuration or the PIN, you must have previously configured the mail server settings under Administration > Settings > System Settings > Mail Server Configuration.

- Ensure TFTP is enabled on the Prime Infrastructure server by choosing Administration > Settings > System Settings > Server, then clicking Enable under TFTP. TFTP is enabled by default.

Refer Release Notes for Cisco Network Plug and Play to know the devices and the corresponding software images supported for APIC-EM.

For more Details on all the supported devices and the corresponding sysObjectIDs, see Cisco Prime Infrastructure 3.0 Supported Devices.

**Related Topics**

- Plug and Play Workflow
- Plug and Play Profiles

**Prerequisites for Deploying Bootstrap Configuration into a Device**

### Table 32-1  Supported Devices and Image Versions for (continued)CNS Gateway

<table>
<thead>
<tr>
<th>Supported Devices for Plug and Play</th>
<th>Minimum Software Image Version Supported</th>
<th>Verified Image Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 3560C</td>
<td>Cisco IOS Release 12.2.55(EX) and later</td>
<td>Cisco IOS Release 12.2.55(EX) and later</td>
</tr>
<tr>
<td>Catalyst 4503, 4506, 4507, and 4510 switches and 4000 Series supervisor cards supported: Sup 6E, Sup 6LE</td>
<td>Cisco IOS Release 151-2.SG and later</td>
<td>Cisco IOS Release 151-2.SG and later</td>
</tr>
<tr>
<td>Catalyst 4503, 4506, 4507, and 4510 switches and 4000 Series supervisor cards supported: Sup 7E, Sup 7LE (IOS XE)</td>
<td>Cisco IOS XE Release 03.04.00.SG and later</td>
<td>Cisco IOS XE Release 03.04.00.SG and later</td>
</tr>
<tr>
<td>Catalyst 3650, 3850 switches (IOS XE)</td>
<td>Cisco IOS XE Release 03.02.02.SE and later</td>
<td>Cisco IOS XE Release 03.02.02.SE and later</td>
</tr>
<tr>
<td>Cisco 5760 Wireless LAN Controllers (IOS XE)</td>
<td>Cisco IOS XE Release 03.02.02.SE and later</td>
<td>Cisco IOS XE Release 03.02.02.SE and later</td>
</tr>
</tbody>
</table>

Refer Release Notes for Cisco Network Plug and Play to know the devices and the corresponding software images supported for APIC-EM.

For more Details on all the supported devices and the corresponding sysObjectIDs, see Cisco Prime Infrastructure 3.0 Supported Devices.

**Related Topics**

- Plug and Play Workflow
- Plug and Play Profiles

**Prerequisites for Deploying Bootstrap Configuration into a Device**

To deploy bootstrap configuration into a device in a Prime Infrastructure Server:

- Enable Cipher in Admin mode of the server by entering the following command.
  
  $ ncs run pnp-ciphers enable
  
- Click Enable in the HTTP Forward section of the Administration > Settings > System Settings > Server Settings page.

- If you are going to use email to deliver either the bootstrap configuration or the PIN, you must have previously configured the mail server settings under Administration > Settings > System Settings > Mail Server Configuration.

- Ensure TFTP is enabled on the Prime Infrastructure server by choosing Administration > Settings > System Settings > Server, then clicking Enable under TFTP. TFTP is enabled by default.
Bootstrap Configuration

A bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the Prime Infrastructure gateway (CNS or APIC-EM). Prime Infrastructure provides a standard bootstrap configuration that you can use.

If you are using the DHCP option, you do not need to create a bootstrap configuration. See Using DHCP to Export Bootstrap Configurations.

To create a user-defined bootstrap template, follow these steps:

---

Step 1: Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Bootstrap.

By default, an APIC Bootstrap and Plug and Play Bootstrap template will be displayed. These templates cannot be deleted.

Step 2: Select the specific Bootstrap check-box and click Clone to clone a similar template. This new template will be displayed as APIC Bootstrap_1, APIC Bootstrap_1_1, and so on or Plug and Play Bootstrap_1, Plug and Play Bootstrap_1_1 and so on, depending on the bootstrap you cloned.

Note: You can rename the cloned template. Once renamed, you cannot change the template name again.

Step 3: Click Save.

Step 4: Click the pointer beside the Bootstrap template to view or edit the details.

Step 5: Click Update to save the changes. Click CLI to view the CLI summary.

Step 6: To delete any bootstrap template, select the specific bootstrap template check-box and click Delete.

---

These templates that you create will be saved in PnP Bootstrap Templates (User Defined).

You can choose this newly created bootstrap template when adding a profile instance by selecting the specific bootstrap template from PnP Bootstrap Templates (User Defined). The details will automatically be displayed and will be editable.

You can also use the Configuration > Templates > Features & Technologies > CLI Templates > System Templates-CLI > Plug And Play Bootstrap to create a customized bootstrap template.

The bootstrap configurations that Prime Infrastructure provides have the following content:

- **CNS HTTP Bootstrap**
  
  ```
  ip host OVA-VM-176 10.104.118.176
  cns trusted-server all-agents OVA-VM-176
  cns trusted-server all-agents 10.104.118.176
  cns id Hardware-Serial
  cns id Hardware-Serial event
  cns id Hardware-Serial image
  cns event OVA-VM-176 encrypt keepalive 120 2 reconnect-time 300
  cns exec encrypt 443
  cns config partial OVA-VM-176 encrypt 443
  cns config initial OVA-VM-176 encrypt 443
  ```

- **CNS HTTPS Bootstrap**

---
In the following example, `pi-hateast-151` is the Prime Infrastructure server hostname.

```
crypto pki trustpoint pi-hateast-151
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check crl
quit
```

```
crypto pki certificate chain pi-hateast-151
certificate ca 4CAAA6BE30 0D06092A 864886F7 0D010105
30820122 2A864886 F70D0101 01050003 B2010F00 3082010A 02820101 00877ECC 98CFD97 92BA4B4C 8611B089 E4453714 844F2DE2 C944F907 D53BB92A 0162A25C 007F2E5F 51CA9A930 8EADFB3A 165DA325 004FCFEE 2DD09A9B 8B165508
```

```
quit
```

```
exit
```

```
ip host pi-hateast-151 10.104.119.151
cns trusted-server all-agents pi-hateast-151
cns trusted-server all-agents 10.104.119.151
cns id hardware-serial
cns id hardware-serial event
cns event pi-hateast-151 encrypt keepalive 120 2 reconnect-time 60
cns exec encrypt 443
cns image server https://pi-hateast-151/cns/HttpMsgDispatcher status
https://pi-hateast-151/cns/HttpMsgDispatcher
```

- **APIC-EM HTTP Bootstrap**
  - pnp profile network-pnp
  - transport http ipv4 <APIC-EM server IP>

- **APIC-EM HTTPS Bootstrap**
  - crypto ca trustpoint <APIC-EM Server IP>.cisco.com
  - enrollment mode ra
  - enrollment terminal
After you create a deployment profile and export it, you can download this certificate directly from Prime Infrastructure. If executing the bootstrap in a device, only the last two commands are required because the APIC-EM server will install certificates directly on the device.

Methods of Installing Bootstrap Configurations

A bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the Prime Infrastructure gateway (CNS or APIC-EM). The bootstrap configuration can be installed on the devices using any of the bootstrap delivery methods that Prime Infrastructure supports:

- Export and download the bootstrap—If you have access to the device console, you can export the bootstrap, and then copy and paste the bootstrap configuration to the device. See Exporting the Bootstrap Configuration.
- Deploying bootstrap configuration through terminal server. See Deploying the Bootstrap Configuration Using Terminal Server.
- Export and save the bootstrap to a USB flash drive—You can save the bootstrap configuration to a USB drive with the file name `ciscortr.cfg`. Connect the USB drive to the device, and then boot the device. The device will retrieve the bootstrap configuration from the USB drive. See Exporting the Bootstrap Configuration Using TFTP.
- Email the bootstrap. See Emailing the Bootstrap Configuration.
- DHCP options based on the server you specified. See Using DHCP to Export Bootstrap Configurations.
  - For CNS gateway—DHCP option 150
  - For APIC-EM—DHCP option 43. You can configure option 43 on the APIC-EM server IP under DHCP Configuration. When a device gets its IP address from DHCP, it will get the bootstrap configuration also.
- Mobile application—You can use the Cisco Network Plug and Play mobile application.

Related Topics

- Prerequisites for Deploying Bootstrap Configuration into a Device
Chapter 32  Configuring Plug and Play

Methods of Installing Bootstrap Configurations

- Bootstrap Configuration
- Exporting the Bootstrap Configuration
- Exporting the Bootstrap Configuration Using TFTP
- Emailing the Bootstrap Configuration
- Using DHCP to Export Bootstrap Configurations

Exporting the Bootstrap Configuration

You can export a bootstrap configuration and then manually apply the bootstrap on the device. After the bootstrap configuration is applied, the Plug and Play deployment is initiated and the administrator can view the configuration status on Prime Infrastructure.

Step 1  Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.
Step 2  From the Plug and Play Profiles page, select a profile from the list.
Step 3  Click Profile Instances.
Step 4  Click Export Bootstrap > Download Bootstrap, then click OK.
Step 5  After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.

Related Topics
- Exporting the Bootstrap Configuration Using TFTP
- Emailing the Bootstrap Configuration
- Using DHCP to Export Bootstrap Configurations
- Bootstrap Configuration

Deploying the Bootstrap Configuration Using Terminal Server

If you have enabled the check box Enable Terminal Server while creating a Plug and Play profile you can deploy bootstrap config:

Step 1  Select the devices from the Plug and Play profile.
Step 2  Click Deploy button.
Step 3  Click OK in the pop up dialogue box to trigger a job to execute the bootstrap on to the device directly by using Terminal Server.

You can check the status of the PnP Terminal Server job on the Job Dashboard.

The APIC will provision the device when the job is executed successfully. The device will be added to the Prime Infrastructure inventory once the device is provisioned.
Chapter 32      Configuring Plug and Play

Methods of Installing Bootstrap Configurations

Exporting the Bootstrap Configuration Using TFTP

If you are using a CNS gateway only for Plug and Play, you can use the TFTP protocol to deliver the bootstrap configuration to the Prime Infrastructure TFTP server. You can specify the file name that should be created on the TFTP server; this file is used by the auto-install enabled devices to get the IP address and other Prime Infrastructure details through the DHCP. In the DHCP server, the TFTP server must be configured as the Prime Infrastructure TFTP server. For more information, please see Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E.

| Step 1 | Choose **Configuration > Plug and Play > Dashboard** and in the **Home** tab, click **PnP Profiles**. |
| Step 2 | From the Plug and Play Profiles page, select a profile from the list. |
| Step 3 | Click **Profile Instances**. |
| Step 4 | Click **Export Bootstrap > TFTP**. |
| Step 5 | After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated. |

Related Topics

- Emailing the Bootstrap Configuration
- Bootstrap Configuration
- Emailing the PIN for the Bootstrap Configuration
- Using DHCP to Export Bootstrap Configurations

Emailing the Bootstrap Configuration

You can email the bootstrap configuration and then manually apply the bootstrap on the device. After the bootstrap configuration is applied, the automated deployment is initiated. The administrator can view the configuration status on Prime Infrastructure.

**Note**

Before you can email the bootstrap configuration, you must set the email settings under **Administration > Settings > System Settings > Mail and Notification > Mail Server Configuration**.

To email the bootstrap configuration to the operator:

| Step 1 | Choose **Configuration > Plug and Play > Dashboard** and in the **Home** tab, click **PnP Profiles**. |
| Step 2 | From the Plug and Play Profiles page, select a profile from the list. |
| Step 3 | Click **Profile Instances**. |
| Step 4 | Click **Export Bootstrap > Email Bootstrap**. |
| Step 5 | Enter the email address to which the bootstrap configuration is be sent, then click **OK**. |
| Step 6 | After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated. |
Emailing the PIN for the Bootstrap Configuration

Prime Infrastructure generates a random Personal Identification Number (PIN) per device. This PIN can be used to identify the device and the Plug and Play profile (bootstrap configuration) associated with it. After the pre-provisioning tasks are complete, the administrator must use the Email PIN option (available in the pre-provisioning task of the Prime Infrastructure) to email the unique PIN to the deployment engineer. During installation, the deployment engineer uses this PIN to download the bootstrap configuration from the server.

To deliver the PIN for the bootstrap configuration:

**Step 1** Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

**Step 2** From the Plug and Play Profiles page, select a profile from the list.

**Step 3** Click Profile Instances tab.

**Step 4** Click CNS Email PIN.

**Step 5** Enter the email address to which the PIN should be sent and click OK.

**Step 6** Use one of the following methods to apply the bootstrap configuration:

- If you are applying the bootstrap configuration using the deployment application, the Prime Infrastructure Plug and Play deployment application communicates to the Prime Infrastructure and applies the bootstrap configuration on the device.

- If you are manually applying the bootstrap configuration using the PIN:
  - Use the PIN to download the configuration from the Prime Infrastructure Plug and Play gateway: https://<pnp-gateway-server>/cns/PnpBootstrap.html. You can also register the ISR’s serial number during this process.
  - Apply the bootstrap configuration on the device manually, using a console or USB flash.

For detailed information about Plug and Play deployment, see the Cisco Plug and Play Application User Guide.

**Step 7** After the bootstrap configuration is applied, the Plug and Play deployment is initiated.
Using DHCP to Export Bootstrap Configurations

To use the DHCP option to export a bootstrap configuration, you must have the following configuration on your devices:

- For CNS gateway—DHCP option 150
  ```
  ip dhcp pool <DHCP pool name>
  network <subnet> <subnet mask>
  default-router <default gateway>
  option 150 ip <prime_infrastructure_server_IP>
  ```

- For APIC-EM—DHCP option 43
  ```
  ip dhcp pool <DHCP pool name>
  network <subnet> <subnet mask>
  default-router <default gateway>
  option 43 ascii "5A1D;B2;K4;I<APIC-EM_server_IP>;J80"
  ```

Sample DHCP Server Settings

If you select the DHCP-based method to deliver the Plug and Play Profile, you must configure the DHCP server to redirect the switch to the TFTP server by entering the commands described in Table 32-2.

This method is not supported for HTTPS with the Encrypt CNS commands. It is supported with the HTTP CNS commands.

The DHCP-based method follows these steps:

1. The new switch contacts the DHCP server. You must configure the DHCP server to redirect the switch to the TFTP server. See Table 32-2 for more information.
2. The DHCP server points the switch to the new TFTP server where the Plug and Play bootstrap profile resides.
3. The switch loads the bootstrap configuration file, boots up, and then contacts the Plug and Play Gateway.

### Table 32-2 DHCP Server Settings

<table>
<thead>
<tr>
<th>Command to Enter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp pool PNP</td>
<td>Creates a DHCP pool named PNP.</td>
</tr>
<tr>
<td>network 10.106.190.0 255.255.255.224</td>
<td>Defines the network 10.106.190.0 and subnet mask 255.255.255.224. DHCP uses this pool of IP addresses to assign an IP address to the new device.</td>
</tr>
<tr>
<td>default-router 10.106.190.17</td>
<td>Configures the default route 10.106.190.17 on the new device.</td>
</tr>
<tr>
<td>option 150 ip 10.77.240.224</td>
<td>Specifies that the TFTP server IP address 10.77.240.224 is the Prime Infrastructure server IP address.</td>
</tr>
</tbody>
</table>

**Note**
Cisco does not support these non-Cisco DHCP products. However if you are using other DHCP servers please note the following:

- Both the CNS-based Cisco Plug and Play Agent and the APIC-EM based Cisco Open Plug-N-Play Agent use a VPN-ID option (Option 221) of "Mgmt-intf" in their DHCP packets. An enterprise level DHCP server will not be able to process these packets without properly handling that VPN-ID.
Both the CNS-based Cisco Plug and Play Agent and the APIC-EM based Cisco Open Plug-N-Play Agent expect the TFTP server address to be returned as a string. Enterprise level DHCP servers return Option 150 as an IP address, and Option 66 as a string.

Both the CNS-based Cisco Plug and Play Agent and the APIC-EM based Cisco Open Plug-N-Play Agent expect a default route (Option 33). Enterprise level DHCP servers return Option 33 as a default route, not just the address of the router as provided by Option 3.

Related Topics
- Viewing Plug and Play Dashboard
- Plug and Play Profiles
- Bootstrap Configuration
- Methods of Installing Bootstrap Configurations

Verifying Device Status

Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Status Information. The device details (Serial ID, hostname, IP address, type, profile name, location), current and post Plug and Play statuses, and the graphical representation of the provisioning status are displayed in a List view.

Click Map in the upper right corner to view the device details and their statuses in map view. See Integrating Map View.

You can choose Administration > Dashboards > Job Dashboard > User Jobs > Post PnP Status to view the status of post Plug and Play configuration job on a device.

You can provision the device profiles again by selecting a device from the list and clicking the Reset button. Choose Configuration > Plug and Play > Dashboard > Device Status. The Reset button is enabled only for devices that have been successfully provisioned or when the provisioning has failed. It is not enabled for devices that show the provisioning status as pending.

You can also reset the device profiles in the profile instance page by choosing Configuration > Plug and Play > Dashboard > Profiles > Router Policies. On resetting a device, provisioning status will be reset to pending.

If Prime Infrastructure is integrated with GA2 or APIC-EM, on resetting the device, it will first be reloaded if the provisioning had failed earlier.

Integrating Map View

You can view the details in a map view in any of the following ways:
- Choose Configuration > Plug and Play > Dashboard and click Monitoring tab.
- Choose Configuration > Plug and Play > Dashboard and click Home tab. Click Status Information and click Map from the upper right corner of the Device Status page.
- Choose Configuration > Plug and Play > Dashboard and click Home tab. Click Locations.
<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click to view the map in full screen.</td>
</tr>
<tr>
<td>2</td>
<td>You can perform zooming operations using mouse or keyboard. With keyboard, click the + or - signs to zoom in or zoom out. With mouse, use the mouse scroll wheel to zoom in or zoom out or double-click to zoom in.</td>
</tr>
<tr>
<td>3</td>
<td>Click to view the provisioning status of the device in detail.</td>
</tr>
<tr>
<td>4</td>
<td>Click to view the sites that do not have geographical coordinates specified.</td>
</tr>
<tr>
<td>5</td>
<td>Click to view the devices that are not mapped to any location. Drag and drop the devices to a location in the map. The device automatically gets mapped to that location group.</td>
</tr>
<tr>
<td>6</td>
<td>Toggle the button to enable edit mode. Once enabled, you can drag and drop the unmapped devices to a location in the map. Before you map a device to a location, create location groups. See Using Location Groups.</td>
</tr>
<tr>
<td>7</td>
<td>Select a location from the list.</td>
</tr>
<tr>
<td>8</td>
<td>Click to view the cluster details. A cluster represents two or more locations in a geographical area. Hover the mouse over the site to view the number of devices mapped to it. Click the number hyperlink to view the device details.</td>
</tr>
<tr>
<td>9</td>
<td>Click List to view the Device Status page.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Verifying Device Status
- Deleting Plug and Play Profiles
- Viewing Plug and Play Dashboard
- Plug and Play Profiles
- Activating Device Profiles
- Bootstrap Configuration
Deleting Plug and Play Profiles

If you are using APIC-EM for Plug and Play, you might need to delete a plug and play profile that is incorrect or outdated.

**Step 1** Execute the following command from the router CLI to remove the Plug and Play profile from the router:
```
no pnp profile plug_and_play_profile_name
```

**Step 2** Delete the provisioning profile by choosing **Configuration > Plug and Play > Dashboard** and click **PnP Profiles**. Select a Plug and Play profile, click **Profile Instances**, then delete the required provisioning profile.

**Step 3** Choose **Configuration > Plug and Play > Dashboard** and click **PnP Profiles**. Select the Plug and Play profile you want to delete, then click **Delete**.

**Related Topics**
- Viewing Plug and Play Dashboard
- Plug and Play Profiles
- Activating Device Profiles
- Bootstrap Configuration
- Verifying Device Status
Managing Device Inventory

This part contains the following sections:

- Viewing Devices
- Updating Device Inventory
- Managing and Monitoring Compute Resources
- Maintaining Software Images
- Working with Device Configurations
- Grouping Devices, Ports and Data Center
Viewing Devices

- Viewing Network Devices
- Viewing Compute Devices

Viewing Network Devices

From the Inventory > Device Management > Network Devices (or Monitor > Managed Elements > Network Devices) page, you can view device inventory and device configuration information. The Network Devices page contains general administrative functions and configuration functions as described in Table 34-1.

Table 34-1 Network Devices Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Location in Inventory &gt; Device Management &gt; Network Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage devices</td>
<td>You can add, edit, delete, sync, and export devices, add and delete devices from groups and sites, and perform a bulk import.</td>
<td>Buttons are located at the top of the page. For more details, see Adding Devices Manually, Exporting Devices, and Importing Devices from Another Source in Related Topics. You can add, edit, delete, sync, and export default and child VDCs. For more details on VDC, see Adding Devices Manually in Related Topics.</td>
</tr>
<tr>
<td>View basic device information and collection status</td>
<td>View basic device information such as reachability status, IP address, device type, and collection status.</td>
<td>Hover your mouse cursor over icon in the IP Address column and click the icon to access the 360° view for that device (see Getting Device Details from the Device 360° View in Related Topics). Hover your mouse cursor over the Last Inventory Collection cell and click the icon to view errors related to the inventory collection.</td>
</tr>
<tr>
<td>Manage device groups</td>
<td>By default, Cisco Prime Infrastructure creates dynamic device groups and assigns devices to the appropriate Device Type folder. You can create new device groups that appear under the User Defined folder.</td>
<td>Displayed in the left pane of the Network Devices Page.</td>
</tr>
</tbody>
</table>
### Table 34-1  
**Network Devices Tasks (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Location in Inventory &gt; Device Management &gt; Network Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add devices to site groups</td>
<td>After you set up a site group profile, you can add devices to it.</td>
<td>Add to Group button located at the top of the Network Devices page under Groups &amp; Sites.</td>
</tr>
<tr>
<td></td>
<td>To add devices to site groups in Network Devices page, add them to Group and then select site group.</td>
<td>Add to Group drop down list available under Add device.</td>
</tr>
<tr>
<td></td>
<td>To add devices to site maps, go to the Maps &gt; Site Map.</td>
<td>Add to Group drop down list available under Edit device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> A device can belong to one site group hierarchy only.</td>
<td>Click Bulk Import and import devices using CSV file.</td>
</tr>
<tr>
<td>View device details</td>
<td>View device details such as memory, port, environment, chassis view and interface information.</td>
<td>Click a Device Name to view the Device Details page for that device.</td>
</tr>
<tr>
<td></td>
<td>View device information and status, and associated modules, alarms, neighbors, and interfaces, managed VDCs, VDC details. For more information, see Getting Device Details from the Device 360° View.</td>
<td>Hover your mouse cursor over a device IP address and click the information icon.</td>
</tr>
<tr>
<td>Create and deploy configuration templates</td>
<td>You can configure device features on the selected device. You can also view the list of applied and scheduled feature templates that were deployed to the device.</td>
<td>Click a Device Name, then click the Configuration tab. For more information about configuring features on a device, see Configuring Device Features in Related Topics</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> From the Network Devices page, it may not be possible to add configuration for a few controller features. In this case, use the Design page and create a new Template and deploy to the device.</td>
<td></td>
</tr>
<tr>
<td>View device configurations</td>
<td>View archived configurations, schedule configuration rollbacks, and schedule archive collections.</td>
<td>Click on a Device Name, then click the Configuration Archive tab.</td>
</tr>
<tr>
<td>View software images</td>
<td>You can view the recommended software image for a single device, and then import or distribute that image. If you want to distribute a software image to multiple devices, see Deploying Software Images to Devices in Related Topics.</td>
<td>Click on a Device Name, then click the Image tab. Scroll down to Recommended Images to view the recommended image for the device that you selected. Prime Infrastructure gathers the recommended images from both Cisco.com and the local repository. You can import the recommended image (see Importing Software Images in Related Topics) or distribute (see Deploying Software Images to Devices in Related Topics) the recommended image.</td>
</tr>
</tbody>
</table>
Chapter 34  Viewing Devices

Viewing Compute Devices

Compute Devices provide a consolidated view of all the devices that provide compute capability within a Data Center. You can manage Cisco UCS devices in the same way other network devices are managed, see Viewing Network Devices in Related Topics. From the Inventory > Device Management > Compute Devices (or Monitor > Managed Elements > Compute Devices) page, you can view device inventory information for the physical devices such as UCS B-series, C-series and E-series devices that support data center virtualization and the data center components as described in Table 34-2.

Table 34-1  Network Devices Tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>Location in Inventory &gt; Device Management &gt; Network Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>View interface details</td>
<td>You can view the description, admin status, and operational status of the interface.</td>
<td>Click on a Device Name, then click the Configuration tab. Click Interfaces to view the interface details.</td>
</tr>
<tr>
<td>View and modify TrustSec configuration</td>
<td>You can view and modify the TrustSec configuration of a TrustSec-based device.</td>
<td>Click on a Device Name, then click the Configuration tab. Click Security &gt;TrustSec &gt; Wired 802_1x.</td>
</tr>
<tr>
<td>Chassis View</td>
<td>You can view a graphical representation of the front or back panel of a device.</td>
<td>Click a device to view the Chassis View in the Device Details page for that device. Note Note The following devices can support chassis view: All AireOS Wireless LAN Controllers, Cisco 5760 LAN controller, Catalyst 3850 Switch, Catalyst 3860 Switch and Catalyst 4K Switch.</td>
</tr>
<tr>
<td>View VDC details</td>
<td>You can view the summary, VDC resources, top 3 CPU utilization and allocated CPU, and VDCs managed.</td>
<td>Click on a Device Name, then click the VDC tab.</td>
</tr>
</tbody>
</table>

Related Topics

- Viewing Compute Devices
### Chapter 34      Viewing Devices

#### Table 34-2  Compute Devices Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>List View</th>
<th>Detailed View</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Data Center</td>
<td>The list view shows the number of clusters, number of hosts, total number of VMs, status of VMs, discovery source and monitoring status of the data center.</td>
<td>Click the data center name in the <strong>List View</strong> to view the properties of the data center. In the detailed view, you can see General, Clusters, Hosts, and VMs tabs. The <strong>General</strong> tab shows the properties of data center displayed in the list view. The <strong>Clusters</strong> tab shows the number of clusters available in this data center. The <strong>Hosts</strong> and <strong>Virtual Machines</strong> tabs shows the details of operational status, CPU usage, memory usage, CPU contention, and swap rate of the hosts and VMs, respectively. The Host section displays the details of hosts available in the selected data center and additional information on the installed operating systems. The Virtual Machine section shows the details of the virtual machines available in the selected data center and additional information on the memory granted and disk rate.</td>
</tr>
<tr>
<td>View Clusters</td>
<td>The list view shows the hosts count, number of VMs, power on/off status of VMs and discovery sources.</td>
<td>Click the cluster name in the <strong>List View</strong> to view the properties of the cluster. In the detailed view, you can see General, Alarms, Hosts, and Virtual Machines tabs. The <strong>General</strong> tab shows the properties of clusters displayed in the list view. The <strong>Alarms</strong> tab shows the alarms associated with the Cluster. The Hosts and Virtual Machines tabs show the operational status, CPU usage and memory usage of the hosts and VMs, respectively.</td>
</tr>
</tbody>
</table>
Table 34-2  Compute Devices Tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>List View</th>
<th>Detailed View</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Hosts</td>
<td>The list view shows the hosts count, number of VMs, power on/off status of VMs, discovery sources, host name, physical server, physical device name, alarm, and alarm count.</td>
<td>Click the host name in the list view to view the properties of the host. &lt;br&gt; &lt;br&gt; You can view the performance metrics of host and its parent cluster. The performance metrics shows a graphical representation of CPU utilization, memory usage and network performance. &lt;br&gt; &lt;br&gt; In the detailed view, you can also see the General, Virtual Machine, Alarm and User Defined Field tabs.  &lt;br&gt; &lt;br&gt; The <strong>General</strong> tab shows the blade server name and UCS device name if the host is installed on a UCS blade server managed by Prime Infrastructure.  &lt;br&gt; &lt;br&gt; The <strong>Virtual Machine</strong> tab shows the operational status, CPU and memory usage details of VMs that belong to the host.  &lt;br&gt; &lt;br&gt; The <strong>User Defined Field</strong> tab allows you to update the user defined values.</td>
</tr>
<tr>
<td>View Virtual Machines</td>
<td>The list view shows the operational status, host name, operating system, monitoring status, discovery source, alarm (maximum severity) and alarm count of the VM.</td>
<td>Click the VM name in the List View to view the properties of the VM. &lt;br&gt; &lt;br&gt; You can view the performance metrics of VM and its parent host and cluster. The performance metrics of VM shows a graphical representation of CPU, memory, disk and network usage. The performance metrics of parent host shows a graphical representation of CPU and memory usage. The performance metrics of parent cluster shows a graphical representation of CPU and memory usage. &lt;br&gt; &lt;br&gt; In the detailed view, you can also see the Virtual Machine General, Hosts General, Alarm and User Defined Field tabs.  &lt;br&gt; &lt;br&gt; The <strong>Virtual Machine General</strong> tab shows the properties of VM. The <strong>Host General</strong> tab shows physical server details if the host is installed on a UCS blade server. The <strong>Alarm</strong> tab shows the operational status, CPU and memory usage details of the VM. The <strong>User Defined Field</strong> tab allows you to update the user defined attributes that store additional information about devices, such as device location attributes.</td>
</tr>
</tbody>
</table>
### Creating User Defined UCS Groups

In addition to viewing the compute device details, you can also create user defined UCS sub-groups. Hover your mouse over the expand icon next to User Defined UCS and click **Add SubGroup**. See *Creating Device Groups* in Related Topics. However, these User Defined UCS group is not reflected in *Monitor > Monitoring Tools > Alarms and Events*.

**Related Topics**
- Creating User Defined UCS Groups
- Creating User Defined Hosts and VMs

### Creating User Defined Hosts and VMs

You can create user defined Hosts and VMs Sub-groups similar to device groups. Hover your mouse over the expand icon next to User Defined Hosts and VMs and click **Add SubGroup**. See *Creating Device Groups* in Related Topics. However, these User Defined Hosts and VMs group are reflected in *Monitor > Monitoring Tools > Alarms and Events* to monitor the alarms or events from any member of this group.

**Related Topics**
- Creating User Defined UCS Groups
CHAPTER 35

Cisco Prime Infrastructure provides two ways to discover the devices in your network:
- **Quick**— Allows you to quickly discover the devices in your network based on the SNMP community string, seed IP address, and subnet mask you specify. Choose **Inventory > Device Management > Discovery**, then click **Quick Discovery**. See **Running Quick Discovery**.
- **Regular**— Allows you to specify protocol, credential, and filter settings, and schedule the discovery job. You can also apply to the added devices any credential profiles you have created. See **Changing Discovery Settings** and **Using Credential Profiles**.

### Changing Discovery Settings

To change the discovery settings, follow these steps:

**Step 1** Choose **Inventory > Device Management**, then click **Discovery Settings**.

**Step 2** Click **New**. Enter the settings as described in **Table 6-1**.

**Step 3** Click one of the following:
- **Save** to save the settings.
- **Run Now** to save the settings and immediately start the discovery job.

**Related Topics**
- **Running Quick Discovery**
- **Running Discovery**
- **Scheduling Discovery Jobs**
- **Monitoring the Discovery Process**
- **Updating Device Inventory Manually**
- **Using Credential Profiles**
**Scheduling Discovery Jobs**

To create a discovery job and then schedule it to run at a future time, follow these steps:

**Step 1** Choose **Inventory > Device Management**, click **Discovery Settings**, then click **New**.

**Step 2** Enter the required settings, then click **Save**.

**Step 3** In the Discovery Settings, select the discovery job that you just created, then click **Schedule**.

**Step 4** Enter the schedule information, then click **Save**.

**Related Topics**

- Running Quick Discovery
- Running Discovery
- Monitoring the Discovery Process
- Updating Device Inventory Manually
- Using Credential Profiles

**Monitoring the Discovery Process**

To monitor the discovery process, follow these steps:

**Step 1** Choose **Inventory > Device Management > Discovery**.

**Step 2** Select the running discovery job for which you want to see details.

**Discovery Protocols and CSV File Formats**

Prime Infrastructure uses the following protocols to discover devices:

- Ping Sweep
- Cisco Discovery Protocol (CDP)
- Routing Table
- Address Resolution Protocol (ARP)
- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)

You can import a CSV file to add data for the protocols. Table 35-1 describes the CSV file format for each of the protocols.

**Note**

You can import a CSV file if you are using a supported version of Mozilla Firefox only.
Chapter 35  Updating Device Inventory

### Updating Device Inventory Manually

We recommend that you run discovery to update your device inventory. However, you can also add devices manually, if needed.

To update the device inventory manually, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Inventory &gt; Device Management &gt; Network Devices</strong>, then click <strong>Add</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the required parameters.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Add</strong> to add the device with the settings that you specified.</td>
</tr>
</tbody>
</table>

**Note**

As part of the SNMP read-write credential verification on the device, a log message appears in the managed device indicating there was a configuration change from the IP address of the Prime Infrastructure server during the inventory task.

### Editing Device Inventory Manually

To edit any parameters in the devices that are already added, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Inventory &gt; Device Management &gt; Network Devices</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the device that you need to edit and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the required parameters.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Update</strong> or <strong>Update &amp; Sync</strong> to update the device with the required settings.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Running Quick Discovery
- Running Discovery
- Scheduling Discovery Jobs

---

### Table 35-1  Discovery Protocols and CSV File Formats

<table>
<thead>
<tr>
<th>Protocol</th>
<th>CSV File Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping sweep</td>
<td>Any valid IP address and subnet mask, separated by a comma. You can specify multiple networks in a single discovery by adding additional rows.</td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP)</td>
<td>Any valid IP address and the hop count, separated by a comma.</td>
</tr>
<tr>
<td>Routing table</td>
<td>Any valid IP address and the hop count, separated by a comma.</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP)</td>
<td>Any valid IP address and the hop count, separated by a comma.</td>
</tr>
<tr>
<td>Border Gateway Protocol (BGP)</td>
<td>Seed device IP address for any device that is BGP enabled.</td>
</tr>
<tr>
<td>Open Shortest Path First (OSPF)</td>
<td>Seed device IP address for any device that is OSPF enabled.</td>
</tr>
</tbody>
</table>
Importing Device Inventory

If you have another management system to which your devices are to be imported or if you want to import a spreadsheet that contains all your devices and their attributes, you can import device information in bulk into Prime Infrastructure.

To import device inventory, follow these steps:

**Step 1** Choose Inventory > Device Management > Network Devices, then click Bulk Import.

**Step 2** Click the link to download a sample file that contains all of the fields and descriptions for the information that must be contained in your imported file.

**Step 3** Click Browse to navigate to your file, then click Import and wait for the import to complete. (To check the status of the import, choose Administration > Job Dashboard > Jobs > User Jobs > Import).

Using Credential Profiles

Credential profiles are collections of device credentials. The credentials stored in a credential profile can include SNMP, Telnet, SSH and HTTP/HTTPS credentials. Credential profiles allow you to apply a set of credentials to a device or a group of devices, instead of entering them manually for each device.

Choose Inventory > Device Management > Credential Profiles to add, edit, delete or copy credential profiles. You can apply a credential profile during device discovery, when manually adding a device, or during bulk import of devices.

**Related Topics**

- Changing Discovery Settings
- Updating Device Inventory Manually
- Importing Device Inventory
- Adding Credential Profiles
- Editing Credential Profiles
- Deleting Credential Profiles
- Copying Credential Profiles.

Adding Credential Profiles

To add a credential profile, follow these steps:

**Step 1** Go to Inventory > Device Management > Credential Profiles.

**Step 2** Click Add.

**Step 3** Enter the Profile Name and Description under the General Parameters.

**Step 4** Enter valid credentials and other values in the SNMP, Telnet/SSH and HTTP/HTTPS fields.
For Cisco WLC only SNMP parameters are mandatory, whereas for Cisco ASR and Cisco ISR both SNMP and Telnet/SSH parameters are mandatory.

You cannot apply a credential profile to a device unless the profile has at least an SNMP read credential.

Step 5 Click Save Changes.

Related Topics
- Using Credential Profiles
- Editing Credential Profiles
- Deleting Credential Profiles
- Copying Credential Profiles

Editing Credential Profiles

To edit a credential profile:

Step 1 Go to Inventory > Device Management > Credential Profiles.
Step 2 Choose the profile and Click Edit.
Step 3 Click Profile Details and enter valid credentials and other values in the SNMP, Telnet/SSH and HTTP/HTTPS fields.
Step 4 (Optional) Click Device List to view the devices associated with the selected profile.
Step 5 Click Save to update the profile of all associated devices or Click Save and Sync to update and synchronize the devices with the updated profile.

Note During bulk edit of devices:
- The credential profile associated with the devices with different credential profile will get lost.
- The manually updated parameters like Telnet and HTTP parameters will be applied to all of the selected devices.

Related Topics
- Using Credential Profiles
- Adding Credential Profiles
- Deleting Credential Profiles
- Copying Credential Profiles
- Viewing Devices Associated with a Credential Profile
Deleting Credential Profiles

To delete a credential profile:

**Step 1** Go to **Inventory > Device Management > Credential Profiles**.
**Step 2** Select the credential profile to be deleted.
**Step 3** Click **Delete**.

You cannot delete a credential profile until you have removed all device-to-profile associations. You can remove these associations using the device edit page under **Inventory > Device Management > Network Devices**.

Related Topics
- Using Credential Profiles
- Adding Credential Profiles
- Editing Credential Profiles
- Copying Credential Profiles
- Viewing Devices Associated with a Credential Profile

Copying Credential Profiles

To copy a credential profile:

**Step 1** Go to **Inventory > Device Management > Credential Profiles**.
**Step 2** Choose a credential profile, then click **Copy**.
**Step 3** Enter the Profile Name and Description under the **General Parameters**.
**Step 4** Enter valid values in SNMP, Telnet/SSH and HTTP/HTTPS fields.
**Step 5** Click **Save Changes**.

Related Topics
- Using Credential Profiles
- Adding Credential Profiles
- Editing Credential Profiles
- Deleting Credential Profiles
- Viewing Devices Associated with a Credential Profile

Viewing Devices Associated with a Credential Profile

To view the credential profile associated with a device:
Step 1  Choose **Inventory > Device Management > Credential Profiles**.

Step 2  Choose a credential profile, then click **Edit**.

Step 3  Click the Device List to view the devices associated with the selected profile.

---

**Troubleshooting Unmanaged Devices**

A device can be unmanaged by Prime Infrastructure, as indicated in the Admin Status column in the **Inventory > Device Management > Network Devices**, if any of the following are true:

- You have exceeded the maximum number of managed devices allowed for your license. If you need additional information about licensing, see the following:
  - *Cisco Prime Infrastructure 3.0 Quick Start Guide*—contains descriptions of the different licenses, how to order licenses, and license entitlement.
  - *Cisco Prime Infrastructure 3.1 Administrator Guide*—contains information about managing licenses, troubleshooting licensing issues, and verifying license details.

- The device is enabled for switch path tracing only.

- The wrong device credentials were entered into Prime Infrastructure so that Prime Infrastructure was unable to contact the device. In this case, the Reachability column in **Inventory > Device Management > Network Devices** is red and indicates the device is unreachable.

If the Device Type column in the **Inventory > Device Management > Network Devices** displays *Unknown* for a device, Prime Infrastructure does not support the device. You can check if support for that device type has been added to Prime Infrastructure by choosing **Administration > Software Update**, then clicking **Check for Updates**.
Managing and Monitoring Compute Resources

Managing VMware Vcenter Server

You can add, delete, edit, sync, and bulk import VMware Vcenter servers and also view the complete inventory of compute resources like data center, cluster, hosts and virtual machines (VMs).

Related Topics
- Adding VMware Vcenter Servers
- CSV File Requirements for Importing Vcenter

Adding VMware Vcenter Servers

You can manage a Vcenter server by manually adding a Vcenter server.

Before you Begin
You must add Data Center Hypervisor license for collecting the inventory of Vcenter server. For adding Data Center Hypervisor license, see Adding a License to Access Features in Related Topics.

To add a Vcenter Server:

Step 1 Choose Inventory > Compute Devices > Discovery Sources.
Step 2 Click Add Device.
Step 3 Enter the following parameters in the Add Discovery Source page.
  - Protocol—HTTP/HTTPS.
  - Server—Host Name/IP address of Vcenter.
  - Port—443 for HTTPS; 80 for HTTP.
  - User Name/Password—Vcenter credentials.
Step 4 (optional) Click Verify Credentials to confirm the Vcenter credentials before adding Vcenter.
Step 5 Click Add.

You can view the inventory collection status of the manually added Vcenter server in the Discovery Sources page. Add the Data Center Vcenter license, if the Virtual Inventory Collection Status shows “No License.”
CSV File Requirements for Importing Vcenter

To use a CSV file to import Vcenter from another source into Prime Infrastructure, you can download a sample template by choosing Inventory > Compute Devices > Discovery Sources, then clicking Bulk Import. Click the link to download a bulk virtual discovery sample template.

For full inventory collection in Prime Infrastructure, you must provide the following values in the CSV file:

- Discovery Source
- Discovery Source Password
- Discovery Source Port
- Discovery Source User Name
- Protocol

Monitoring Performance of Compute Resources

Prime Infrastructure monitors the managed compute resources by periodically polling the devices.

Prime Infrastructure supports periodic polling of a predefined set of key performance indicators (KPIs) related to CPU, memory, disk and network for monitoring the health of the virtual elements. Prime Infrastructure does not poll the VM directly, but it gets the data periodically from the Vcenter via the application programming interfaces (APIs). The default polling interval is 5 minutes. You can change the polling interval as described below.

Setting Polling Interval for Monitoring Compute Resources

To set the polling interval:

**Step 1** Choose Administration > Settings > System Settings > Datacenter Settings.

**Step 2** Choose the Polling Interval from the drop-down list.

**Step 3** Click Save.
Polling can be enabled/disabled on data center, cluster and host. The children of the entity selected for polling would be automatically selected for polling. For example, if polling is enabled on a cluster, then all the hosts and VM belonging to that host would be automatically selected for polling. Click the Start Monitoring button on Data Center, Cluster and Hosts list view in Compute Device screen to enable polling.

Related Topics
- Monitoring Clusters

## Monitoring Clusters

If monitoring is enabled from parent (data center or cluster) then it cannot be stopped from child (host or cluster). But you can stop the monitoring enabled from child (host, cluster) by clicking Stop Monitoring from parent (data center, cluster).

To monitor a cluster:

**Step 1** Choose Inventory > Device Management > Compute Devices.

**Step 2** Click Clusters in the Compute Resources pane.

**Step 3** Choose the clusters and click Start Monitoring.

Related Topics
- Setting Polling Interval for Monitoring Compute Resources
CHAPTER 37

Maintaining Software Images

Overview of Software Image Management

Manually upgrading your devices to the latest software version can be error prone and time consuming. Cisco Prime Infrastructure simplifies the version management and routine deployment of software updates to your devices by helping you plan, schedule, download, and monitor software image updates. You can also view software image details, view recommended software images, and delete software images. The software image management page provides a consolidated view of the various aspects of image management such as software image management lifecycle widget, software image summary, and job details.

Prime Infrastructure stores all of the software images for the devices in your network. The images are stored according to the image type and version.

Before you can upgrade software images, you must configure your devices with Telnet or SSH credentials. Also SNMP read-write community strings that match the community strings entered when the device was added to Prime Infrastructure must be configured.

To ensure that there are no SNMP views blocking access to the CISCO-FLASH-MIB, remove the following command from the configuration for all routers and switches (if present) on which you want to download a software image:

```
snmp-server view ViewName ciscoFlashMIB excluded
```

SSH or Telnet must be configured for importing the images from a device.

Related Topics

- Software Image Management Processes and Supported Devices
- NotePrime Infrastructure does not support software image distribution on Cisco Catalyst 4500 devices configured with a redundant supervisor engine.
- Configuring Software Image Management Server for Image Distribution
- Managing Software Images
- Importing Software Images
- Importing Software Images to the Virtual Image Repository
- Changing Software Image Requirements
- Distributing Software Images to Devices
Software Image Management Processes and Supported Devices

Table 37-1 describes the different processes involved in managing software images and whether the processes are supported in the Unified Wireless LAN Controllers and devices.

<table>
<thead>
<tr>
<th>Software Image Management Processes</th>
<th>Description</th>
<th>Unified WLCs</th>
<th>3850 Cisco IOS XE 3.2.2</th>
<th>5760 Cisco IOS XE 3.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image import from device</td>
<td>Ability to import software image from devices that are already managed by Prime Infrastructure. The software image can then be distributed to other devices.</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Image import from file</td>
<td>Ability to import software image from known location on a file server to Prime Infrastructure. The software image can then be distributed to other devices.</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Image import from URL</td>
<td>Ability to import software image from network accessible locations (URI/URL) to Prime Infrastructure. The software image can then be distributed to other devices.</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Image import from Protocol</td>
<td>Ability to import software image from an FTP location to Prime Infrastructure. The software image can then be distributed to other devices.</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>
### Table 37-1 Software Image Management Processes and Supported Devices (continued)

<table>
<thead>
<tr>
<th>Software Image Management Processes</th>
<th>Description</th>
<th>Unified WLCs</th>
<th>3850 Cisco IOS XE 3.2.2</th>
<th>5760 Cisco IOS XE 3.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image upgrade/distribution</td>
<td>Ability to upgrade software image on the managed devices from Prime Infrastructure. This allows you to upgrade the software image for multiple devices based on demand or at a later point in time as scheduled. The feedback and status are displayed during the upgrade and devices can be restarted, if required. In large deployments, you can stagger reboots so that the service at a site is not completely down during the upgrade window.</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Image recommendation</td>
<td>Ability to recommend a compatible image for the devices that are managed from Prime Infrastructure and downloaded from Cisco.com.</td>
<td>Not supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Image upgrade analysis</td>
<td>Ability to analyze the software images to determine the hardware upgrades required before you can perform the software upgrade.</td>
<td>Not supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**Note**
Prime Infrastructure does not support software image distribution on Cisco Catalyst 4500 devices configured with a redundant supervisor engine.
Prime Infrastructure supports software image distribution on Cisco Catalyst 6000 devices with dual supervisors; Prime Infrastructure distributes the software image on both the active and the standby supervisor engine.

Setting Image Management and Distribution Preferences

By default, Prime Infrastructure does not collect and store device software images when it gathers inventory data from devices.

To set image management and distribution preferences:

**Step 1** Choose **Administration > Settings > System Settings > Image Management**.

**Step 2** To have Prime Infrastructure automatically retrieve and store device images when it collects device inventory data, check **Collect images along with inventory collection**.

**Step 3** Select other options as necessary. Hover your mouse cursor over the information icon to view details about the options.

The Config Protocol Order field specifies the order in which the protocol is used. For example, if SSH is listed before Telnet, SSH is used first, and Telnet is used next.

**Step 4** Click **Save**.

**Step 5** Choose **Inventory > Device Management > Software Images** and click **Links** adjacent to **Software Image Repository** under **Useful Links** section. Click **Image Dashboard** icon in the top-right corner of Software Image page to view all of the software images retrieved by Prime Infrastructure. The images are organized by image type and stored in the corresponding software image group folder.

Configuring Software Image Management Server for Image Distribution

You can add and configure a software image management server for distributing images to a group of devices in a particular location.

Before you begin, you must create location groups in **Inventory > Group Management > Network Device Groups** to add sites in software image management server.

**Step 1** Choose **Administration > Servers > Software Image Management Servers**.

**Step 2** Click the Add icon and enter the Server Name, IP Address and Sites Served details of the software image management server. Active protocols are configured by specifying the above details.

You can add multiple sites in one software image management server. You can add a maximum of three servers.

**Step 3** Click **Save**.

**Step 4** Click **Manage Protocols**.

**Step 5** Click the Add icon and enter the software image management protocol details.
Prime Infrastructure does not support TFTP protocol for image distribution using software image management server. The supported protocols are SFTP, SCP, and FTP.

**Step 6**
Click Save.

**Note**
When a distribution job is triggered using the Software Image Management Server (an external server), the protocol orders, which is configured on the Manage Protocols and Image Management Settings page is picked up by the common protocol which is applicable to the respective devices. For example, if the distribution is triggered using the local file server, then the distribution job running is based on the image management protocol order.

**Related Topics**
- Creating Location Groups

## Managing Software Images

The software image dashboard displays the top software images used in your network and allows you to change image requirements, see the devices on which an image is running, and distribute images.

**Step 1**
Choose **Inventory > Device Management > Software Images**.

**Step 2**
Click **Software Image Repository** under **Useful Links**.

**Step 3**
Click **Image Dashboard** in the top-right corner of Software Image page.

**Step 4**
Click a software image name to display details about the image.

**Step 5**
Do any of the following:
- Change image requirements. See **Changing Software Image Requirements**.
- View the devices on which the software image is running.
- Distribute the image. See **Distributing Software Images to Devices**.

## Importing Software Images

It can be helpful to have a baseline of your network images by importing images from the devices in your network. You can also view recommended software images from Cisco.com.

By default, Prime Infrastructure does not automatically retrieve and store device images when it collects device inventory data. (You can change this preference as described in **Note**Prime Infrastructure does not support software image distribution on Cisco Catalyst 4500 devices configured with a redundant supervisor engine.)

Based on a device’s capabilities, Prime Infrastructure can use different protocols (SCP, TFTP, FTP) to import images from devices. For better reliability and security, we recommend you use secure protocols only (SFTP, SCP) for importing software images. We do not recommend using TFTP or FTP.

To import a software image:
Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click **Add/Import**.

Step 3 Enter the source from where to import the software image. You can specify any one of the following sources:

- **Device**—An existing device. For Cisco Catalyst 3850 Ethernet Stackable Switch and Cisco 5760 Series Wireless Controller there are two modes for importing the software images.
  - **Install mode**—When the device is running in install mode, the running image will be “packages.conf”. Prime Infrastructure does not support importing of any image in install mode.
  - **Bundle mode**—When the device is running in Bundle mode, the running image will be in “.bin” format. Prime Infrastructure supports importing of any image in bundle mode.
  - You can check the running image in one of the following ways:
    a. Choose **Inventory > Network Devices**, click the device name and click **Image** tab in the device page.
    b. Use Show version command in device CLI.

- **URL**—Specify the FTP URL from where you can import the software image. You can use an HTTP URL where user credentials are not required.

- **Protocol**—Specify the FTP location from where you want to import a software image. User credentials are required. The FTP protocol only is supported.

- **File**—A local file on the client machine.

**Note** Prime Infrastructure supports to import Non-Cisco standard image.

**Note** For wireless LAN controllers, you can import software images from a file or a URL or using FTP Protocol only. For more information about Software Image Management Processes and Supported Devices, see **Table 37-1**.

Step 4 Specify **Collection Options** and enter the required information.

Step 5 Specify the **Schedule** when to import the image file. You can run the job immediately or schedule it to run at a later time.

Step 6 Click **Submit**.

Step 7 Choose **Administration > Dashboards > Jobs Dashboard > User Jobs > SWIM Collection** to view the status about the image collection job. The Duration field is updated after the job completes.

**Related Topics**

- Distributing Software Images to Devices
- Importing Software Images to the Virtual Image Repository
Importing Software Images to the Virtual Image Repository

You can use the Prime Infrastructure Virtual Image Repository (VIR) to automatically retrieve and store device images from specified URLs or files. You can schedule these downloads to occur regularly. Currently, the VIR supports FTP or HTTP downloads only.

To import software images to the VIR:

**Step 1** Choose **Inventory > Device Management > Virtual Image Repository**. The page lists the number of images currently retained in the repository.

**Step 2** Click **Import**.

**Step 3** Specify the **Source** from which to import the software image. You can specify one of the following sources:
- **URL**—Specify the FTP or HTTP URL from which to import the software image. You can use an HTTP URL where user credentials are not required.
- **File**—A local file on the client machine.

**Step 4** Click **Collection Options** and then enter the required information.

**Step 5** Click **Schedule** and specify the schedule on which to import image file. You can run the collection job immediately or schedule it to run at a later time. You can also schedule the job to recur automatically.

**Step 6** Click **Submit**.

**Step 7** Choose **Administration > Dashboards > Jobs Dashboard > User Jobs > SWIM Collection** to view the status about the image collection job. The Duration field is updated after the job completes.

**Related Topics**
- Distributing Software Images to Devices
- Importing Software Images

Changing Software Image Requirements

To change the RAM, flash, and boot ROM requirements that a device must meet for a software image to be distributed to the device:

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** In the **Useful Links** section, click **Link** adjacent to **Software Image Repository** to view the **Software Image Summary** page.

**Step 3** Navigate to and select the software image for which you want to change requirements, then click **Image Details**.

**Step 4** Modify the necessary fields, then click **Save**. Your changes are saved in the required software version.

**Step 5** Click **Restore Defaults**, if you want to retain the previous image details.
Distributing Software Images to Devices

You can distribute a software image to a device or set of similar devices in a single deployment. Prime Infrastructure verifies that the device and software image are compatible.

Based on a device’s capabilities, Prime Infrastructure can use different transport protocols (SCP, TFTP, FTP, SFTP) to distribute images to devices. For better reliability and security, we recommend you to use secure protocols only (SFTP, SCP) for distributing software images. If you choose SCP protocol for the image distribution, ensure that the device is managed in Prime Infrastructure with full user privilege (Privileged EXEC mode), otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

We do not recommend using TFTP or FTP. If you choose TFTP protocol for the image distribution and if the device and the server are in different subnet, the image should be copied within the specified session time limit (one hour) which is maintained by the application otherwise the distribution will fail due to timeout error.

For Software Image Distribution to work efficiently, the device and server from which the distribution is performed must be in the same geographical location or site. The Software Distribution job would return error if the distribution takes more time due to network slowness or low speed.

Note

To ensure that there are no SNMP views blocking access to the CISCO-FLASH-MIB, remove the following command from the configuration for all routers and switches (if present) on which you want to download a software image:

```
snmp-server view ViewName ciscoFlashMIB excluded
```

Step 1  Choose Inventory > Device Management > Software Images.

Step 2  Click Distribute in the Software Image Management Lifecycle widget.

Step 3  In the Image Selection window, choose the software images that you want to distribute.

Step 4  Click the Device Selection tab, and choose the devices that you want to distribute the image. By default, the devices for which the selected image is applicable are shown.

Step 5  Click the Image Details Verification tab and click the image row to do the following:

- Choose the image name in the Distribute Image Name field to change your selection and pick a new image, then click Save.

- Choose the value displayed in the Distribute Location field, select a new location in which to store the software image, then click Save.

- Choose the value displayed in the Software Image Management Server field, then click Save. You can choose either a Local file server or one of the servers created under Administration > Servers > Software Image Management Servers.

The Status and Status Message fields display the validity of the selections you made. For example, if the status is green, there is adequate space available to store the image on the specified location on the device.

Step 6  Click the Image Deployment tab and set the image deployment options as required:

- Backup Current Image—Before distributing new images, import the running images from the device to software images repository page.

- Insert boot command—To set the boot variable in the device boot path list.
• Activate—To enable the Activate option, you must check the **Insert Boot Command** check box.
  
  – Activate OFF—New image will be distributed and boot variable is set in device boot path list. Device will not be rebooted in this mode and will continue to run with the running image.
  
  – Activate Sequential—Once the image distribution is completed for all the selected devices, the device will reboot sequentially.
  
  – Activate Parallel—Once the image distribution is completed for all the selected devices, the devices will reboot simultaneously.

• Erase Flash Before Distribution—Clears the flash memory before image distribution if there is no sufficient space in the device.

• Continue on Failure—If the image distribution fails for one image, the next device in queue will be picked up for distribution.

• TFTP Fallback—It prompts the device to reload the current running image from the TFTP server location during image distribution failure.

**Step 7**

Prime infrastructure allows you to use a maximum of one Local file server and three Software Image Management Servers for software image distribution. Each server can distribute the image to five devices at one instance. When the image distribution is completed for one device, the next subsequent device will be taken up for the image distribution. Click the **Schedule Distribution** tab and specify the schedule options, then click **Submit**.

The distribute image job is non-repetitive. The details about the image distribution job is displayed in the Software Image Management dashboard. You can also view the image distribution job details from **Administration > Dashboards > Job Dashboard > User Jobs > SWIM distribution**. The **Duration** field is updated after the job completes.

---

**Distributing Software Images to Wireless Devices**

You can view the **Device Upgrade Mode** option only during image upgrade for Cisco 5760 Series Wireless Controller and Cisco Catalyst 3850 Ethernet Stackable Switch. **Table 31-3** describes the possible device upgrade options and the corresponding image format for Cisco 5760 Series Wireless Controller and Cisco Catalyst 3850 Ethernet Stackable Switch.

<table>
<thead>
<tr>
<th>Device Upgrade Mode</th>
<th>Device Image Format Before Distribution</th>
<th>Device Image Format After Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Install mode to Bundle mode</td>
<td>packages.conf</td>
<td>.bin</td>
</tr>
<tr>
<td>Change Install mode to Currently Existing mode</td>
<td>packages.conf</td>
<td>packages.conf</td>
</tr>
<tr>
<td>Change Bundle mode to Currently Existing mode</td>
<td>.bin</td>
<td>.bin</td>
</tr>
<tr>
<td>Change Bundle mode to Install mode</td>
<td>.bin</td>
<td>packages.conf</td>
</tr>
</tbody>
</table>

If the image distribution status is “Success”, you can check the new image version using any of the following options:

• Choose **Inventory > Network > Network Devices**.
  
  – View the **Software Version** column in the Network Devices page.
  
  – Click the device name and click the **Image** tab.
Use the `show version` command in the device CLI.

Activating Software Images

After successful distribution of the images to all the devices, you must apply the image and reboot the device. Prime Infrastructure provides the following two options to activate the images:

- **Activate From Library**—Allows you to activate an image already available in the device flash memory. Table 37-2 lists the supported device types and the image family.
- **Activate from Completed Distribution Jobs**—Allows you to activate the images based on the recent successful or partially successful Image Distribution jobs.

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** Click **Activate** in the Software Image Management Lifecycle widget.

**Step 3** In the **Activation Source** window, click the **Activate from Library** radio button or **Activate from Completed Distribution Jobs** radio button as required.

**Step 4** If you choose **Activate from Completed Distribution Jobs**, click the **Job Selection** tab. All successful and partially successful jobs are displayed.

**Step 5** In the **Job Selection** window, choose the successful image distribution jobs that you want to activate.

**Step 6** Click the **Activate Preview** tab, and choose the devices that you want to activate the image.

After selecting the devices, go to **Step 11**.

**Step 7** If you choose **Activate from Library** in the **Activation Source** window, click the **Image Selection** tab.

**Step 8** In the **Image Selection** window, the supported images are filtered and displayed from the **Software Image Summary** page. Choose the software images that you want to distribute.

**Step 9** Click the **Device Selection** tab, and choose the devices that you want to activate the image.

By default, the devices for which the selected image is applicable are shown.

**Step 10** Click the **Activate Image** tab, and verify whether the selected devices and software images are mapped correctly for activation.

**Step 11** Click the **Activate Job Options** tab, and choose the required Activate Job options.

If you choose the ISSU option from the **Activate** drop-down list, the software image in the device will get upgraded without need for rebooting the device. The ISSU option supports only Catalyst 4000, Catalyst 6000 and Nexus devices.

**Step 12** Click **Submit** to activate the software image in the selected devices.

Supported Image Format for Stack Devices

Prime Infrastructure supports only .tar images for upgrade and downgrade for stacked devices. Stack device do not support .bin format. The list of supported stack devices are:

- Stack of CBS3100 switch modules
- Cisco Catalyst Switch Module 3110X for IBM Blade Center
- Cisco Catalyst Blade Switch 3120X for HP
Viewing Recommended Software Images from Cisco.com

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** Click **Software Image Repository** under **Useful Links**.

**Step 3** Click the software image which you want to change requirements.

**Step 4** Choose the devices which you want to distribute the image from the **Device List** and click **Distribution New Version**.

**Step 5** **Select Image from Local Repository** to select an image stored locally. Then, under Local Repository:
- Select the **Show All Images** check box to display all images available in the Prime Infrastructure repository.
- Unselect the **Show All Images** check box to display the software images applicable to the selected device.

**Step 6** Select the image to distribute, then click **Apply**.

**Step 7** Choose the image name in the Distribute Image Name field to change your selection and pick a new image, then click **Save**.

**Step 8** Specify Distribution Options. You can change the default options in **Administration > Settings > System Settings > Image Management**.

**Step 9** Specify schedule options, then click **Submit**.

Analyzing Software Image Upgrades

Prime Infrastructure can generate an Upgrade Analysis report to help you determine prerequisites for a new software image deployment. These reports analyze the software images to determine the hardware upgrades (boot ROM, flash memory, RAM, and boot flash, if applicable) required before you can perform the software upgrade.

The Upgrade Analysis report answers the following questions:
- Does the device have sufficient RAM to hold the new software?
Analyzing Software Image Upgrades

- Is the device’s flash memory large enough to hold the new software?
- Is the software image suitable/applicable for the device?

To analyze software image upgrades:

Step 1 Choose Inventory > Device Management > Software Images.
Step 2 Click Upgrade Analysis.
Step 3 Choose the source of the software image that you want to analyze.
Step 4 Select the devices on which to analyze the software image.
Step 5 Select the images to analyze for the selected devices.
Step 6 Click Run Report.
Working with Device Configurations

Cisco Prime Infrastructure archives device configurations and provides information such as the date of last configuration change, status of the configuration jobs, and allows you to compare current and previous configurations. Prime Infrastructure also allows you to roll back to a previously saved configuration in the archive if a configuration deployment fails.

- Configuration Archives
- Changing Prime Infrastructure Device Configuration Settings
- Comparing Current and Previous Device Configurations
- Scheduling Configuration Archive Tasks
- Overview of Device Configurations
- Configuration Rollbacks
- Rolling Back Device Configuration Versions
- Deleting Device Configurations

Configuration Archives

Prime Infrastructure attempts to collect and archive the following device configuration files:

- Startup configuration
- Running configuration
- VLAN configuration, if configured

A configuration archive is created if there is a change between the last archived configuration and the current running configuration only. You can specify how Prime Infrastructure archives the configurations:

- On demand—You can have Prime Infrastructure collect the configurations of selected devices by choosing Inventory > Device Management > Configuration Archive and selecting the option to schedule the archive immediately.
- Scheduled—You can schedule when Prime Infrastructure collects the configurations of selected devices and specify recurring collections by choosing Inventory > Device Management > Configuration Archive, then clicking Schedule Archive.
You can schedule to have Prime Infrastructure copy the running configuration to the startup configuration by choosing **Inventory > Device Management > Configuration Archive**, then clicking **Overwrite**.

- During inventory—You can have Prime Infrastructure collect device configurations during the inventory collection process. See **Changing Prime Infrastructure Device Configuration Settings** for more information.
- Based on Syslogs— If device is configured to send syslogs, when there is any device configuration change, Prime Infrastructure collects and stores the configuration.

### Downloading Configuration Files

You can download the Startup and Running configuration files of up to a maximum of 1000 devices at a time, to your local system.

**Step 1** Choose **Inventory > Device Management > Configuration Archive**.

**Step 2** Select the device for which you want to download configuration files.

**Step 3** From the **Export Latest Archive** drop-down list, select one of the following options to download the configuration files:

- **Sanitized**—The device credential password will be masked in the downloaded file.
- **Non-Sanitized**—The device credential password will be visible in the downloaded file.

The Non-Sanitized option appears based on the user permission set in Role Based Access Control (RBAC).

You can also download the configuration files by doing the following:

- Click the device for which you want to download configuration files in the **Inventory > Device Management > Configuration Archive** page or Click the device for which you want to download configuration files in the **Inventory > Device Management > Network Devices** page and click **Configuration Archive** tab.

  - Click the expand icon.
  - Click **Details**.

Select **Sanitized** or **Non-Sanitized** from the **Export** drop-down list.

### Changing Prime Infrastructure Device Configuration Settings

By default, Prime Infrastructure has the following configuration settings:

- Does not back up the running configuration before pushing configuration changes to a device.
- Does not attempt to roll back to the previously saved configuration in the archive if the configuration deployment fails.
- When pushing CLI to a device, uses 5 thread pools.

To change the default configuration settings:

**Step 1** Choose **Administration > Settings > System Settings**, then click **Configuration**.
Changing Prime Infrastructure Configuration Archive Collection Settings

By default, Prime Infrastructure has the following Configuration Archive collection settings:

- Collects device configuration after Inventory Sync.
- Does not collect device configuration based on syslog events.

To change the default configuration settings:

Step 1 Choose Administration > Settings > System Settings, then click Configuration Archive.

Step 2 Select the Archive Configuration on receiving configuration change events check box so that Prime Infrastructure can collect and store the configuration based on syslog configuration change events. For more information about the supported Syslog formats, see Supported Syslog Formats for Configuration Archive Collection Settings.

Note This feature is not supported for WLC, because WLC does not send any syslog message for configuration changes.

Step 3 Click Save.

Supported Syslog Formats for Configuration Archive Collection Settings

The following are the supported Syslog formats. Prime Infrastructure collects the configuration details if the device syslog matches any one of the following conditions:

- Message Type is any one of the following:
  OIR-6-INSNACRD, SNMP-5-COLDSTART, SYS-5-RELOAD,
  CPU_REDUN-6-BOOTED_AS_ACTIVE, CPU_REDUN-5-SWITCHOVER, SYS-5-ONLINE,
  OIR-6-INSNACRD, CPU_REDUN-6-RUNNING_CONFIG_CHG,
  CPU_REDUN-5-RCSF_SYNCED, CPU_REDUN-6-STARTUP_CONFIG_CHG,
  CPU_REDUN-5-STARTUP_CONFIG_SYNCED, PIX-5-111005, SYS-5-CONFIG_L,
  SYS-5-CONFIG_M, SYS-5-CONFIG_NV, SYS-5-CONFIG_NV_M, SYS-6-CFG_CH,
  SYS-3-CPUHOG, IP-4-DUPADDR, FW-3-FTP_SESSION_NOT_AUTHENTICATED,
  FW-3-FTP_PRIV_PORT, FW-3-SMTP_INVALID_COMMAND, FW-3-HTTP_JAVA_BLOCK,
  FW-4-ALERT_ON, FW-4-ALERT_OFF, FW-4-HOST_TCP_ALERT_ONLOG_WARNING,
  FW-4-UNBLOCK_HOST, FW-2-BLOCK_HOST, SYS-2-MALLOCFAIL, LINK-3-UPDOWN,
  FW-6-SESS_AUDIT_TRAIL, PIX-6-302001, PIX-6-302002, PIX-6-304001,
Comparing Current and Previous Device Configurations

To compare a current device configuration with a previous version:

**Step 1** Choose **Inventory > Configuration Archive**.

**Step 2** Click the expand icon for the device whose configuration you want to view. Then click the expand icon again to view the specific configuration version that you want to compare.

**Step 3** In the Compare With column, choose the configuration for which you want to compare the configuration that you selected in the previous step.

The color key at the bottom of the report shows the differences between the configurations you selected.

Scheduling Configuration Archive Tasks

When you choose **Inventory > Device Management > Network Devices**, click on a device name, then click the **Configuration Archive** tab, Prime Infrastructure allows you to schedule the following configuration archive tasks:
Overview of Device Configurations

You can change a device’s configuration in two ways:

- **Inventory > Device Management > Network Devices**—To change the configuration of a single device. See Changing a Single Device Configuration.

- **Configuration > Templates**—To change the configuration of more than one device and apply a common set of changes, use a configuration template to make the changes.

Prime Infrastructure provides the following default configuration templates:

- CLI templates—CLI templates are user-defined and created based on your own parameters. CLI templates allow you to select the elements in the configurations. Prime Infrastructure provides variables which you replace with actual values and logic statements. You can also import templates from Cisco Prime LAN Management System. See CLI Templates.

- Feature and technology templates—Feature templates are configurations that are specific to a feature or technology in a device’s configuration. See Features and Technologies Templates.

- Composite templates—Composite templates are two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices. See Composite Templates.

Changing a Single Device Configuration

**Step 1** Choose **Inventory > Device Management > Network Devices**, then click a device name. The device details appear in the lower part of the page.

**Step 2** Click the **Configuration** tab. The Feature Selector displays the values, organized into features, for the device that you selected.

**Step 3** Select the feature that you want to change, then make the necessary changes.

**Step 4** Click **Save** to save your configuration changes in the Prime Infrastructure database. (To view the status of the configuration change, choose **Administration > Jobs**.)
Adding a Wireless LAN Controller

The Cisco Unified Wireless Network (CUWN) solution is based on Wireless LAN Controllers running Airespace Operating System. The wireless LAN controller models include 2100, 2500, 4400, WiSM/WiSM2 (6500 service module), 5500, 7500, 8500. In this solution, access points tunnel the wireless traffic to the controllers through CAPWAP.

The Cisco Unified Access (UA) Wireless Solution is new architecture that provides a converged model where you can manage your wired and wireless network configurations in the same place. This solution includes the 3850 series switch with integrated wireless support. The solution also includes the 5760 series wireless controller, which can act as an aggregation point for many 3850 switches. This platform is based on IOS-XE, so the command structure is similar to other IOS products. In this solution, the wireless traffic can terminate directly on the 3850 switch, so that it can be treated in a similar mode to a wired connection on the switch.

---

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  Click Add Device. The Add Device page appears.
Step 3  In the Add Device page, enter the necessary parameters.
Step 4  Click Add.

---

Changing Wireless LAN Controller Configuration Settings

---

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  Expand Device Type, and then click Wireless Controller.
Step 3  Select the controller that you want to change. The Network Devices page contains configuration functions at the bottom of the page. For details, see Monitoring Network Devices.
Step 4  Click the Configure tab, then make the necessary changes.
Step 5  Click Save.

---

Rebooting Controllers

---

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  Expand Device Type, and then click Wireless Controller.
Step 3  Select the check box(es) of the applicable controller(s).
Step 4  From the Reboot drop-down list, choose Reboot Controllers.

Note  Save the current controller configuration prior to rebooting.

Step 5  Select the Reboot Controller options that must be applied.
Configuration Rollbacks

You can change the configuration on a device with a configuration stored in Prime Infrastructure. You can select a single archived version to which you want to “rollback.” During the configuration rollback process, the configuration is converted into a set of commands which are them executed sequentially on the device.

When rolling back a configuration file you can specify the following options:

- The type of configuration file to which to rollback, for example running or startup configuration
- Whether to sync the running and startup configurations after rolling back the running configuration
- If rolling back a startup configuration only, specify to reboot the device so that startup configuration becomes the running configuration
- Before rolling back the configuration, specify whether to create new archived versions. You can also specify whether to continue the rollback if the archived configuration fails.

Rolling Back Device Configuration Versions

You can use Prime Infrastructure to rollback a device’s configuration to a previous version of the configuration.

To roll back a configuration change.

**Step 1** Choose **Inventory > Configuration Archive**.

**Step 2** Click the expand icon for the device whose configuration you want to roll back.

**Step 3** Click the specific configuration version that you want to roll back, then click **Schedule Rollback**.

**Step 4** Specify the rollback and scheduling options.

**Step 5** Click **Submit**.
Deleting Device Configurations

By default, Prime Infrastructure archives up to five device configuration versions for each device for seven days after:

- Every inventory collection
- Prime Infrastructure receives a configuration change event

You cannot delete configuration versions, but older configuration versions are replaced by newer configuration versions.

To change the number of configurations that Prime Infrastructure retains:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; Settings &gt; System Settings, then click Configuration Archive.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter a new value in the Number of Versions field. To archive an unlimited number of configuration versions, unselect the Number of version to retain and Number of days to retain check boxes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>
Grouping Devices, Ports and Data Center

You can create your own logical grouping of devices, ports and data center to enable efficient update and management of your device and data center. For example, you can create a device group that includes devices with a particular module. If you later want to configure a feature related specifically to that module, you use the device group that you created to push the configuration change to all of the devices contained in the group.

Types of Groups

You can use groups to filter views of devices and their associated alarms, control which network topology to view, and perform bulk operations (such as configuration changes and software updates) on sets of devices. Grouping not only saves you time when configuring multiple devices, but it also ensures that configuration settings are applied consistently across your network.

Prime Infrastructure provides the following types of grouping:

- **Device type groups**—Device type groups are device type-based and are not rule-based. The device type groups are not used for network topology maps.
- **User defined groups**—Create your own device-based groups. Device groups are mixed groups which can have dynamic rules and/or manually added members.
- **Location groups**—Create location-based groups. For example, if you have devices that reside in different time zones, you can create location groups based on geographic regions so that the devices in one group can have a different time zone setting from the devices in another group.
- **Port groups**—Create port groups to simplify monitoring and configuring ports.

In smaller deployments where all devices can be configured with the same settings, you may only need to create one general device group. This setup allows you to configure settings for the group, and then apply those settings consistently across all of your devices.

Related Topics

- Creating Device Groups
- Using Location Groups
- Creating Location Groups
- Creating Groups of Ports

Text Part Number:
Accessing Device/Location Groups through Virtual Domains

You can control users access to device groups through virtual domains. For role-based access control (RBAC), you need to create sites and virtual domains. See Related Topics for more details on how to add groups, network devices and users to virtual domains.

You can associate device/location groups to a particular virtual domain and control the user access by assigning the access privilege. If you login to prime Infrastructure with the user name assigned to a particular virtual domain, you can manipulate only the groups associated to that virtual domain. The parent group and other groups that manage the devices associated to the virtual domain can only be viewed and cannot be manipulated.

Related Topics
- Adding Groups to Virtual Domains
- Adding Network Devices to Virtual Domains
- Adding Users to Virtual Domains

Creating Device Groups

Before you create a device group, make sure that you understand the unique properties that you want the group to contain. For example, you may want to set up two device groups that have different authentication settings or different time zone settings.

Note
While there is no limit to the number of rules that you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

To create a device group, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups.

Step 2 In the Device Groups pane on the left, perform one of the following tasks:
- Click the expand icon next to User Defined and click Add SubGroup.
- Click the add icon and choose Create User Defined Group form the drop-down list.

Step 3 Enter the group name and group description, and select a parent group, if applicable.

Step 4 To add devices to a group dynamically,
  a. In the Add Devices Dynamically group box, specify the rules that you want to apply to the devices in the group.
  b. Click Preview to view the devices that are automatically added to the group based on the specified rule and the manually added devices.

You can create a rule using the UDF labels defined in Administration > Settings > System Settings > User Defined Field.
If you want to group devices having specific range of IP addresses, mention the range in square brackets. For example:

- IPv4 — 10.1[01-155].[1-255].[1-255] and 10.126.170.[1-180]
- IPv6 — 2014::5217:[0000-ffff]:fe22:[1e40-1f41]

**Step 5**

To add devices to a group manually,

a. In the **Add Devices Manually** group box, click **Add**.

b. Choose the devices that you want to assign to the group.

**Step 6**

Click **Save** to add the device group with the settings that you specified.

The device group that you created appears under the user-defined groups.

---

**Related Topics**

- Types of Groups
- Using Location Groups
- Creating Location Groups
- Creating Groups of Ports
- Searching Device Groups

---

**Searching Device Groups**

To view the list of device groups to which a device belongs, follow these steps:

**Step 1**

Choose **Inventory > Device Management > Network Devices** or **Inventory > Group Management > Network Device Groups**.

**Step 2**

Enter an IP address or device name in the Search field in the Device Group pane on the left, to view the list of all groups to which the device belongs.

You can also search the group by entering the group name in the search field.

---

**Using Location Groups**

Location groups allow you to group devices by location. You can create a hierarchy of location groups (such as theater, country, region, campus, building, and floor) by adding devices manually or by adding devices dynamically.

A device should appear in one location group only, though a higher level “parent” group will also contain that device. For example, a device that belongs to a building location group might also indirectly belong to the parent campus group.

By default, the top location of the hierarchy is the **All Locations** group. All devices that have not been assigned to a location appear under the Unassigned group under All Locations.
Creating Location Groups

To create a location group, follow these steps:

**Step 1** Choose **Inventory > Group Management > Network Device Groups** or **Inventory > Device Management > Network Devices**.

**Step 2** In the **Device Groups** pane on the left, perform one of the following tasks:
- Click the expand icon next to **Location** and click **Add SubGroup**.
- Click the add icon and choose **Create Location Group** form the drop-down list.

**Step 3** In the **Device Groups** pane on the left, click the expand icon next to **Location** and click **Add SubGroup**.

**Step 4** Enter the group name and group description, and select a parent group, if applicable.

**Step 5** From the **Group Type** drop-down list, choose the type of group such as Default, Campus, Building, Outdoor Area or Indoor Area, so that the same hierarchy gets reflected in the site maps.

If you select Default, the group will not be visible in the site maps.

Make sure that you follow a proper hierarchy while creating sub groups. For example, you can not choose the group type to be floor area for a sub group, when the group type of its parent is Campus.

**Step 6** Check the **Geographical location** check box, to associate a physical location to the location group.

**Step 7** Enter your location in the **Civic Location** field. You can also choose a location by clicking **View Map**. The **GPS (Lat./ Long)** field gets automatically populated with the coordinates based on the selected location.

**Step 8** In the **Add Devices Dynamically** group box, specify the rules that you want to apply to the devices in the group.

**Step 9** In the **Add Devices Manually** group box, choose the devices that you want to assign to the group.

**Step 10** Click **Preview** to view the devices that are automatically added to the group based on the specified rule and the manually added devices.

**Step 11** Click **Save** to add the device group with the settings that you specified.
Location Groups and Wireless Maps

The location groups you create get synchronized with the wireless maps, depending on the selected group such as Campus, Building, Outdoor Area or Indoor Area. Therefore, the location group that you create can be viewed under Maps > Wireless Maps > Site Maps, and similarly the site you create under maps can be viewed under Inventory > Group Management > Network Device Groups, in the hierarchical way.

Importing Location Groups Using CSV File

To import a location group using a CSV file that lists all attributes of the group that you want to add into Prime Infrastructure, follow these steps:

1. Choose Inventory > Group Management > Network Devices, then click Import Groups.
2. Click here to download the Sample Template for CSV file. Make sure that you retain the required information in the CSV file as mentioned in the Template.
3. Click Choose File in the Import Groups dialog box, and select the CSV file that contains the group that you want to import.
4. Click Import.
5. Choose Administration > Dashboards > Job Dashboard and click Import Groups to view the status of the job.

Related Topics
- Creating Location Groups
- Location Groups and Wireless Maps
- Exporting Location Groups as CSV File

Exporting Location Groups as CSV File

To export group information as a CSV file, follow these steps:

1. Choose Inventory > Group Management > Network Devices.
2. Click Export Groups to download the CSV file including the details of all location groups, into your local system.

Related Topics
- Creating Location Groups
- Location Groups and Wireless Maps
• Importing Location Groups Using CSV File

Editing User Defined and Location Groups

You can change the parent group, add devices, and modify device rules using the edit option.

To edit a group follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Inventory &gt; Group Management &gt; Network Device Groups.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Device Groups pane on the left, click the name of the group you want to edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Edit and modify the details. When you are editing a location group, you can change the group type to Campus, if:</td>
</tr>
<tr>
<td></td>
<td>• The group type is Default.</td>
</tr>
<tr>
<td></td>
<td>• The group does not have any subgroups.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Preview to view the updated device details.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save to save the updated device details.</td>
</tr>
</tbody>
</table>

Duplicating User Defined and Location Groups

You can duplicate a group using the Duplicate Group option in quick view. The duplicated group contains all of the values entered by the user in the UI for a group. The populated group name will have a prefix of ‘CopyOf’ by default. You can change the name, if required.

If you duplicate a child group, a copy of child group is created under the same parent group.

To duplicate a group follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Inventory &gt; Group Management &gt; Network Device Groups.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Device Groups pane on the left, click the icon next to the name of the group you want to duplicate.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Duplicate Group and update the device details.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Preview to view the updated device details.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save to save the updated device details.</td>
</tr>
</tbody>
</table>

Device Accessibility in Parent-Child Device and Location Groups

The device inheritance in parent-child user defined and location groups are as follows:

• User Defined Group—When you create a child group under a parent device group, the devices accessible to the child group depend on how you add device to the group:
Chapter 39      Grouping Devices, Ports and Data Center

Hiding Empty Groups

A device or port group might be empty if:

• The group does not have any sub groups and/or members.
• No devices match the rules that you specified while adding dynamically.

By default, Prime Infrastructure displays empty groups. If you do not want to display empty groups, choose Administration > Settings > System Settings > Inventory > Grouping, then uncheck Display groups with no members check box.

Note We recommend that you don’t uncheck this check box when there are more number of groups and devices, because this will reduce the performance of the Prime Infrastructure.

Creating Groups of Ports

Creating a port group helps you simplify monitoring and configuration tasks. For example, you might want to create a port group that contains all WAN ports so that you can easily monitor these key ports. By default, port groups are based on interface type.

Note While there is no limit on the number of rules that you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

To create a port group follow these steps:

Step 1 Choose Inventory > Group Management > Port Groups.
Step 2 In the Port Groups pane on the left, mouse hover the expand icon next to the User Defined group and click Add SubGroup.
Step 3 Enter the name, description, and parent group if applicable.
Step 4 Add ports to the group Manually or dynamically:
  • Manually—Click Add under Add Ports Manually. The ports of the selected device is displayed. Choose the ports for adding to the group based on your needs.
  • Dynamically—You must specify rules to which ports must comply before they are added to this port group, under Add Ports Dynamically. You do not add ports to dynamic groups. Prime Infrastructure adds ports that match the specified rules to the dynamic group.
Creating Device Context or Group Context Port Groups

The Device Context Selection option enables you to group ports for a specific device group.

To create a port group for a specific device or group:

Step 1 Choose Inventory > Group Management > Port Groups.

Step 2 In the Port Groups pane on the left, mouse hover the information icon next to the User Defined group and click Add SubGroup.

Step 3 Enter the name, description, and parent group if applicable.

Step 4 Click the Device Selection drop-down arrow.

Step 5 For creating port groups in device context:
   - Click the Device radio button and select any one of the devices from the list of devices displayed.
   - Adding Port Manually—Click Add under Add Ports Manually. The ports of the selected device is displayed. Choose the ports for adding to the group based on your needs.
   - Adding Port Dynamically—Specify the rules to which ports of the selected device must comply before they are added to this port group. You do not add ports to dynamic groups. Prime Infrastructure adds ports that match the specified rules to the dynamic group
   - Click Preview to view the ports that are automatically added based on the specified rule and the manually added ports, and click Save.

Step 6 For creating port groups in Device Group context:
   - Click the Device Group radio button and select any one of the device groups from the list of device and location groups displayed.
   - Adding Port manually—Click Add under Add Ports Manually. The ports of the selected device is displayed. Choose the ports for adding to the group based on your needs.
   - Adding Port Dynamically—Specify the rules to which ports of the selected device must comply before they are added to this port group. You do not add ports to dynamic groups. Prime Infrastructure adds ports that match the specified rules to the dynamic group
   - Click Preview to view the ports that are automatically added based on the specified rule and the manually added ports, and click Save.

Understanding System Defined Port Groups

Prime Infrastructure supports four types of system defined port groups. As and when new devices are added to the system, the ports of the devices are automatically assigned to the respective groups.

- **Trunk Ports**—Ports that are connected to a Cisco device or other network devices (Switch/Router/Firewall/Third party devices) and operating on “Trunk” mode in which they carry traffic for all VLANs.
• **Link Ports**—Ports that are connected to another Cisco device or other network devices and are operating on “VLAN” mode and are assigned to a VLAN.

• **Access Ports**—Ports that are connected to an end host, IP phone, servers, Access Points (AP) or video end points and operating on “Access” mode in which they carry traffic for only one particular VLAN.

• **Unconnected Ports**—Ports are unconnected if any or all of the below are valid:
  - Not connected to any device.
  - Operational status is down.
  - Administrative status is down.

**Note** The ports in this group can not be deleted and neither can this group be created as a sub group. If the status of a port goes down, it is automatically added to Unconnected Port group.

## Adding Access Points (AP) to Device Group or Location Group

You can add AP under the Device or Location group.

To Add AP to device group:

### Step 1
Choose **Inventory > Group Management > Network Device Groups**.

### Step 2
In the Device Groups pane on the left, mouse hover the expand icon next to a **User Defined** or **Location** and click **Add SubGroup**.

### Step 3
Enter the name, description, and parent group if applicable.

### Step 4
Add APs in one of the following ways:

- **Manually**—Click **Add** under **Add Devices Manually** and select APs to be added to the group, based on your need.

- **Dynamically**—Specify rules to which APs must comply before they are added to this port group. You do not add APs to dynamic groups. Prime Infrastructure adds APs that match the specified rules to the dynamic group.

  If you select any type of location group other than Default, the APs will not be added dynamically.

### Step 5
Click **Preview** to view the APs that are automatically added to the group based on the specified rule and the manually added APs.

### Step 6
Click **Save**.

If the group has 'Unified AP' or 'Third Party AP' as its member, a new tab is added in the right hand table in the Device Work Center, to display the APs.

## Creating Customized Port Groups

You can create a customized, user-defined port group that contains devices or interfaces on which you want to apply configuration changes in one operation.

To create a customized port group follow these steps:
Step 1  Choose Inventory > Group Management > Port Groups.

Step 2  In the Device Groups pane on the left, mouse hover the expand icon next to the User Defined and click Add SubGroup.

Leave the default Parent Group text box entry as User Defined.

Step 3  Enter a group name and description, then add ports manually or dynamically:

- Manually—Click Add under Add Ports Manually. The ports of the selected device is displayed. Choose the ports for adding to the group based on your needs.

- Dynamically—You must specify rules to which ports must comply before they are added to this port group. You do not add ports to dynamic groups. Prime Infrastructure adds ports that match the specified rules to the dynamic group.

The port group that you created appears under the User Defined folder.

Step 4  Click Save.

Grouping Integration with Data Center

In addition to the out-of-box groups for data center and cluster, you can create multiple user-defined groups for VMs and hosts.

To create user defined Hosts and VMs groups, follow these steps:

Step 1  Choose Inventory > Device Management > Compute Devices > User Defined Hosts and VMs.

Step 2  Hover your mouse over the expand icon and click Add SubGroup.

Step 3  Enter the group name and group description, and select a parent group, if applicable.

Step 4  In the Add Devices Dynamically pane, specify the rules that you want to apply to the devices in the group.

Step 5  In the Add Devices Manually pane, choose the devices that you want to assign to the group.

Step 6  Click Preview to view the devices that are automatically added to the group based on the specified rule and the manually added devices.

Step 7  Click Save to add the device group with the settings that you specified.
Visualizing the Network

This part contains the following sections:

- Using Topology Maps
- Using Wireless Maps
Using Topology Maps

Cisco Prime Infrastructure provides a visual map of your network’s physical topology, including the network devices and the links that connect them. The topology maps have indicators that show the current alarm status of network devices and links. Using these network or datacenter topology maps, you can easily monitor your network by viewing alarms in the context of the interconnection between devices.

- Topology Overview
- Viewing Detailed Tables of Alarms and Links
- Determining What is Displayed in the Topology Map
- Getting More Information About Devices
- Getting More Information About Links
- Viewing Fault Information for Devices and Links
- Creating a Topology Dashlet
- Changing the Topology Map Layout
- Saving the Topology Map Layout
- Saving the Topology Map as an Image File
- Creating a Topology Dashlet
Topology Overview

The two types of topology maps are:

- **Network Topology**
- **Datacenter Topology**

Network Topology

Prime Infrastructure topology maps are based on Location and User Defined groups (see “Types of Groups” in Related Topics). Topology maps show the devices in the group as well as any links between the devices.

The links between devices are discovered using the Cisco Discovery Protocol (CDP). If Prime Infrastructure is unable to discover some links, for example, if CDP is disabled on an interface, you can manually add the link to the topology map, and then associate the link with a specific interface on the appropriate managed device.

You can also add “unmanaged devices” or “unmanaged network” icons to a topology map and add links between these unmanaged objects and managed devices in the topology map (see “Adding Unmanaged Devices and Links to Topology Maps” in Related Topics).

You can add autonomous APs to Prime Infrastructure topology maps, but you cannot add Unified APs.

The Network Topology window presents a graphical, topological map view of the devices, the links between them, and the active alarms on the devices or links. The Network Topology window also provides access to information and functions relating to device groups, alarms, and links, and allows you to drill down to get detailed information about the devices displayed in the topology map.

The Network Topology window is accessed from the left sidebar (Maps > Network Topology) and consists of the following panes:

- **Device Groups**—Lists the device groups that exist in the system, both Location-based groups and custom, user-defined Device groups. The groups pane is critical because the content of all the other panes in the Network Topology window (as shown in the figure below) is determined by the group that is selected in the Groups pane. From the Groups pane you can access the central device grouping functionality to create new groups, add devices to groups, and so on. For more information, see “Creating Device Groups” and “Creating Location Groups” in Related Topics.

- **Alarm Summary**—Shows all the current alarms for the selected group, categorized by alarm severity. You can access more detailed alarm information by clicking the Show Alarms Table link at the bottom of the pane or by clicking on an alarm severity category, in which case the alarms table is filtered by the selected severity.

- **Links**—Provides access to the Link Table that lists all the links between devices that are relevant to the selected group and provides additional link information. Selecting a link in the table highlights the link in the topology map.

- **Topology Map**—The central, largest pane in the Network Topology window displays the topology of the selected device group in graphical form. It displays the group’s devices and sub-groups (if any) and the links between them. It also displays the active alarms on the devices or links so that you can easily identify problems in the network. You can drill down from the topology map to detailed information about a device or link in order to troubleshoot problems. You can customize, filter and manipulate the topology map to show exactly the information you need.
**Datacenter Topology**

The data center topology keeps no link idle. The next-generation data center provides the ability to use all links in the LAN topology by taking advantage of technologies such as virtual PortChannels (vPCs). vPCs enable full, cross-sectional bandwidth utilization among LAN switches, as well as between servers and LAN switches.

A port channel bundles up to eight individual interfaces into a group to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

A virtual PortChannel (vPC) allows links that are physically connected to two different devices to appear as a single PortChannel to a third device. The third device can be any other networking device. A vPC allows you to create redundancy by increasing bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

After you enable the vPC function, you create a peer keepalive link, which sends heartbeat messages between the two vPC peer devices.

Virtual Device Context (VDC) enables the virtualization of a single physical device in one or more logical devices. Each of the provisioned logical devices is configured and managed as if it were a separate physical device.

**Related Topics**
- Types of Groups
- Creating a Topology Dashlet
- Creating Device Groups
- Creating Location Groups
- Understanding Topology Map Functions and Icons
- Navigating in Topology Maps
- Topology Map Icons
- Before Using Topology Maps
Understanding Topology Map Functions and Icons

From the Device Group selector on the left, expand the Location or User Defined group and click on a group. By default, the Location > All Locations > Unassigned group contains all devices that you have not assigned to any other location group.

When you select a device group, the topology map for the devices contained in that group is displayed, including any discovered links connecting the devices. Links to devices outside the map are not displayed.

The following options at the of the topology pane provide additional features:

- **Overview**—Displays an overview window in lower right corner of the topology window, which shows the full map and, if you have zoomed in on the map, the currently viewable portion of the map.
- **Search**—To find a specific device in your topology, enter a device hostname or IP address, or substring, for the device in the topology Search field. If a device was moved from its initial deployed location but is still on the network or datacenter, you can use the network or datacenter topology search to locate the device.
- **Layout**—Choose a layout option or specify one of these options:
  - **Incremental Layout**—Choose this option when creating a manual or custom layout to re-render links and clean up overlaps before saving it as a Manual Layout.
  - **Save Current Layout**—Choose this option to save the selected layout for the map.
  - **Load Saved Layout**—Choose this option to load a previously saved layout for this map
- **Create Element**—You can create an unmanaged device (represented by a generic icon) or an unmanaged network (represented by a cloud icon). You can also create links between objects.

To show the interface and link status for a created link, click on the created link that connects one more managed devices, then click **Edit Interface Assignment** to assign the link to the appropriate interface on the managed device.

**Related Topics**

- Navigating in Topology Maps
- Topology Overview

Navigating in Topology Maps

In a topology map, icons represent devices or groups of devices. You can click on the icon for a group to bring up the information summary, which shows the group name and alarm summary. You can view the contents of a group in two ways:

- Click on a device group icon, then in the summary panel that appears, click **Drill Down Group**.
- From the Device Group navigation pane, find the group in the hierarchy and click on the group name.

In addition to the summary information, you can also click on a device or group icon, or a link to get additional tools, such as the device 360° view.

**Related Topics**

- Understanding Topology Map Functions and Icons
- Topology Overview
Topology Map Icons

In topology maps, device icons reflect the device alarm state and correspond to the most severe alarm currently active for the device, which can be minor, major, or critical. Similarly, group icons indicate whether any devices within the group have active alarms.

Click on a device or group icon, or a link to display summary information and additional tools, such as the Device 360° View.

Icons on the topology maps display network fault information:

- If a device is currently down or unreachable, the device icon is gray.
- If a device has an alarm associated with it, an alarm badge is displayed on the device icon on the topology map. The color of the alarm badge corresponds with the alarm severity—minor (yellow), major (orange), or critical (red)—and matches the alarms displayed in the Alarm Browser.
- A link down alarm generates an alarm badge on the associated link in the topology map. After the link up alarm is received, the alarms and corresponding badges are cleared.
- The alarm badges on group icons represent the most severe alarm currently active for any object in the group.

Related Topics

- Topology Overview
- Viewing Fault Information for Devices and Links

Before Using Topology Maps

Before you create or view topology maps:

1. Make sure your devices were successfully added to Prime Infrastructure, as explained in “Validating That Devices Were Added Successfully”.
2. You have created one or more device or location groups. Any devices that you do not assign to a group will appear under the Unassigned device group.

Related Topics

- Validating That Devices Were Added Successfully
- Types of Groups
- Creating Device Groups
- Creating Location Groups
- Topology Overview
Viewing Detailed Tables of Alarms and Links

From the Network Topology window, you can access extended tables that list and provide more information about alarms and links. These extended tables open in a separate browser window.

To open the extended details tables, click the Detach icon below the Groups pane or click on the Show Table link in a specific pane.

The window displaying the extended tables has two tabs: Alarms and Links.

Be aware of the following when working with the extended tables:

- When the extended tables window is open, the Alarms and Links panes in the Network Topology window are disabled. If you click on a disabled pane, the extended tables window is brought to the front. When you close the extended tables window, the panes in the Network Topology window become fully functional again.

- There is synchronization between the data in the extended tables and the data in the corresponding panes in the Network Topology window.

- Alarms in both the Network Topology window and in the extended tables are refreshed based on user preference settings (see “Changing Alarm Display Behavior” and “Customizing the Alarm Summary” in Related Topics).

Related Topics
- Changing Alarm Display Behavior
- Customizing the Alarm Summary
- Topology Overview

Determining What is Displayed in the Topology Map

You have control over the elements displayed in the network topology map, and can customize it to show just the information you want, as explained in the following related topics.

Related Topics
- Displaying Network Elements in the Topology Map
- Viewing the Contents of a Sub-Group in the Topology Map
- Manually Adding Links to the Topology Map
- Adding Unmanaged Devices and Links to Topology Maps
- Changing the Link and Device Types Shown in the Topology Map
- Viewing Port Channel Links using LAG
- Showing and Hiding Alarms, Links, and Labels in the Topology Map
- Isolating Specific Sections of a Large Topology Map
Displaying Network Elements in the Topology Map

The topology map enables you to visualize the topology of a selected device group, which might cover a specific network segment, a customer network, or any other combination of network elements. To determine what is displayed in the topology map, you must select a group in the Groups pane to the left of the topology map. Since grouping is hierarchical, a group might be a “parent group,” meaning that it contains sub-groups. If the selected group contains sub-groups, icons representing the sub-groups are shown in the topology map. These icons can be expanded to display the devices within them.

The topology map only displays devices for which the logged in user has access privileges, based on the virtual domains assigned to that user.

If you encounter topology issues, such as topology components not rendering as expected or component data not being displaying on the map, we recommend that you clear your browser cache and try again.

---

**Step 1** Choose **Maps > Topology Maps > Network Topology or Datacenter Topology**.

**Step 2** In the Groups pane on the left, click on the group you want to display in the topology map.

**Step 3** Customize the topology map to show specific device/link types, add manual links, and so on, as explained in these related topics: “Change Which Link and Device Types are Shown in the Topology Map”, “Manually Add Links to the Topology Map” and “Change the Topology Map Layout”.

After you have displayed the required group in the topology map, you can access additional information about any device or link, as explained in these related topics: “Getting More Information About Devices” and “Getting More Information About Links”.

---

**Related Topics**

- Changing the Link and Device Types Shown in the Topology Map
- Viewing Port Channel Links using LAG
- Manually Adding Links to the Topology Map
- Changing the Topology Map Layout
- Getting More Information About Devices
- Getting More Information About Links
- Determining What is Displayed in the Topology Map
Viewing the Contents of a Sub-Group in the Topology Map

You can expand a sub-group to show its contents within the current context or you can drill down to see the contents of the sub-group independently of the current map context.

In the diagram below, the IL group is expanded.

When expanding sub-groups, be aware that if a device belongs to more than one group, the device will appear in one of the expanded groups only. It will not appear in all of the groups to which it belongs. If your setup has devices that belong to multiple groups, rather view the groups individually in the topology map by selecting them in the Groups pane. This will ensure that you will always see all the devices that belong to a specific group.

Step 1
Choose Maps > Topology Maps > Network Topology or Datacenter Topology.

Step 2
In the Groups pane on the left, click on the group you want to display in the topology map.

Step 3
Click on a sub-group in the topology map.

Step 4
In the displayed popup, click one of the following:

- Drill down group—Displays the sub-group on its own in the topology map, meaning that the currently displayed group is replaced with the selected sub-group. Note that the sub-group name is selected in the Groups pane.
- Expand group—Adds the contents of the sub-group to the current topology map display.

Related Topics
- Determining What is Displayed in the Topology Map
Manually Adding Links to the Topology Map

If you have a link in your network that Prime Infrastructure cannot discover, you can manually draw the link in your topology map. The manually created link is considered a managed link. This is because Prime Infrastructure retrieves the link status from the managed device interfaces to which it is connected.

After you have manually added a link to the topology map, the link will be shown by default whenever the relevant group is selected. The manual link cannot be hidden using the link type filter.

**Step 1**  Choose Maps > Topology Maps > Network Topology or Datacenter Topology.
**Step 2**  Click on Create in the topology toolbar and choose Create Link.
**Step 3**  Click and hold down the mouse on the first device in the topology map and drag it to the second device. A dotted line is created between the two devices indicating a manual link.

Related Topics
- Topology Overview
- Changing the Link and Device Types Shown in the Topology Map
- Viewing Port Channel Links using LAG
- Adding Unmanaged Devices and Links to Topology Maps
- Determining What is Displayed in the Topology Map

Adding Unmanaged Devices and Links to Topology Maps

You can add unmanaged devices and links to your topology maps in order to get a complete view of the network. For example, you can add an “unmanaged device” icon to your topology map to represent a network device that is not managed by Prime Infrastructure but is connected to a managed device, and then manually draw the link in your network topology. You can then assign the manually created link to a specific interface on the managed device so you can see the interface alarm status in the topology map.

Related Topics
- Manually Adding Links to the Topology Map
- Determining What is Displayed in the Topology Map
Chapter 41  Using Topology Maps

Determining What is Displayed in the Topology Map

You can choose to display only certain types of links or devices in the topology map. Click the Filter icon to see a full list of link and device types and select the ones you want to display. If you want to temporarily show or hide links, alarms, or labels, see the related topics.

**Step 1** Choose **Maps > Topology Maps > Network Topology or Datacenter Topology**.

**Step 2** Select the required device group from the Groups pane on the left.

**Step 3** Click the Filter icon in the topology toolbar and choose **Link Types** or **Device Families**.

**Step 4** In the Show Link Types or Show Device Families dialog, select the types of links/devices that you want displayed in the topology map, for example, physical layer links, Ethernet layer links, routers, and so on.

- If a device or link type exists in your network, it will be displayed in the dialog. However, it will be disabled if it is not relevant to the currently selected group.
- If a device or link type does not exist in your network, it will not appear in the dialog.

**Step 5** Click **OK**. Your settings are saved and only the link/device types you selected are displayed.

**Related Topics**

- Topology Overview
- Viewing Port Channel Links using LAG
- Showing and Hiding Alarms, Links, and Labels in the Topology Map
- Determining What is Displayed in the Topology Map

Viewing Port Channel Links using LAG

In Prime Infrastructure, after successful Inventory collection of devices, links are created between the devices forming the physical or Ethernet Interfaces. These Interfaces are aggregated and represented as one, thus forming Port channels. When these Port channels are connected, they form a Link Aggregation Group (LAG) link. You can view the topology representation of the Port channel links and its members.

To view the Port channel links, follow these steps:

**Step 1** Choose **Maps > Topology Maps > Network Topology or Datacenter Topology**.

**Step 2** Click the respective Device Group from the Groups pane on the left. The Unassigned Group page displays the topology representation of all the devices.

**Step 3** Click the Filter icon in the topology toolbar and choose **Link Types**.

**Step 4** Check the **LAG** check box in the Show Link Types dialog.

**Step 5** Click **OK**. The topology map shows the Port channel links between the devices/members.

**Step 6** Click the required link in the topology map to view the links summary information. A popup appears showing the basic link details (such as A side, Z side, Link Type and Alarm Severity).

**Step 7** Click the information icon in the popup to launch the 360° Link view for detailed information about the members and port channel links.
Step 8  Click on the required device in the topology map to view the device summary information (such as host name, IP address, and alarm summary). A popup appears showing basic device information and alarm information for the device.

Step 9  Click View 360 in the popup to launch the Device 360° view for detailed information about the device.

Related Topics
• Topology Overview
• Changing the Link and Device Types Shown in the Topology Map
• Determining What is Displayed in the Topology Map

Showing and Hiding Alarms, Links, and Labels in the Topology Map

Use the Show/Hide settings to temporarily add or remove labels, links, and alarm information to your map.

Step 1  Choose Maps > Topology Maps > Network Topology or Datacenter Topology.

Step 2  Click the Show button in the topology toolbar.

Step 3  Select the items you want displayed in the topology map:
• Labels—Labels associated devices, such as device names.
• Links—Single links between devices.
• Aggregated Links—Links that represent more than one underlying link. They are represented by dotted lines.
• Faults—You can choose to hide fault information altogether, show all fault information or show only faults of a certain severity or higher, as it is a slider widget.

Step 4  Close the Show dialog. Your selections are applied to the topology map.

Related Topics
• Changing the Link and Device Types Shown in the Topology Map
• Determining What is Displayed in the Topology Map

Isolating Specific Sections of a Large Topology Map

In cases where a topology map is displaying thousands of devices, you may want to focus on specific devices or sets of devices. The Overview pane shows you the entire topology map in miniature and lets you select the area you want to display in the large topology map. It also provides an at-a-glance view of the alarm status of the elements in the topology map.

Step 1  Choose Maps > Topology Maps > Network Topology or Datacenter Topology.

Step 2  Click the Overview icon in the topology toolbar. The Overview pane appears at the bottom right of the topology map and displays the following:
• Dot— indicates any network element. The color of the dot indicates the severity of alarms associated with the network element.
• Line— indicates a link. The color of the line indicates the severity of the associated alarm.
• Blue rectangle— indicates the selection area. The area within the rectangle is displayed in the map pane. Handles on the corners enable you to resize the selection area.
• Pan mode cursor— cursor displayed within the selection area. Use this cursor to move the selection area, and thereby view different elements in the map pane.
• Zoom mode cursor— displayed outside the selection area. Use this cursor to define a new selection area or to zoom in on an existing selection area.

**Step 3**
Draw a rectangle by dragging the mouse over the area you want to see in the topology map.

**Step 4**
Click the ‘x’ in the upper right corner to close the Overview pane.

### Related Topics
- Changing the Link and Device Types Shown in the Topology Map
- Determining What is Displayed in the Topology Map

## Getting More Information About Devices

From the topology map, you can drill down to get more information about a device.

**Step 1**
Choose Maps > Topology Maps > Network Topology or Datacenter Topology.

**Step 2**
Click on the required device in the topology map. A popup appears showing basic device information and alarm information for the device.

**Step 3**
Click View 360 to access the Device 360 view for detailed information about the device.

### Related Topics
- Getting More Information About Links
- Viewing Fault Information for Devices and Links

## Getting More Information About Links

The representation of links in the topology map provides some information about the link:
• A solid line represents any type of discovered link between two elements in the topology map.
• A dotted line represents an unmanaged link that has been manually drawn in the topology map.
• A dot-dash line represents an aggregated link (if Aggregated Links is selected in the Show popup).
• An alarm severity badge indicates the highest severity alarm currently affecting the link.

From the topology map, you can drill down to get more information about a link by clicking on the required link in the topology map.
• For simple links, the displayed popup shows the link type and the A-side and Z-side of the link.
For aggregated links, the displayed popup shows a table listing all the underlying links.

**Related Topics**
- Getting More Information About Devices
- Viewing Fault Information for Devices and Links

### Viewing Fault Information for Devices and Links

You can use the topology maps to see the device and link faults in your network. Viewing the physical topology helps you understand the potential impact of the fault on the rest of the network and helps you troubleshoot and fix the issues. Network topology maps also help you see the interconnection between network devices and view details about the interconnections, such as link speed and link types.

If a device or link has an alarm associated with it, an alarm badge is displayed on the device icon or on the link in the topology map. The color of the alarm badge corresponds with the alarm severity—minor (yellow), major (orange), or critical (red)—and matches the alarms displayed in the Alarm Browser.

For groups, the alarm badge represents the most severe alarm that is currently active for any of the group members.

Link-related alarms, such as Link Down, generate an alarm badge on the relevant link in the topology map. After the link up alarm is received, the link alarms and corresponding badges are cleared.

See **Topology Map Icons** for more information about the alarm information that is provided by the icons.

---

**Step 1** Choose **Maps > Topology Maps > Network Topology or Datacenter Topology**.

**Step 2** Select the device group, in either the Locations folder or the Custom folder, which you want to view the network topology. If you did not previously create device groups, all devices will appear in the Locations > Unassigned folder.

Icons appear on the devices and links indicating critical, major, minor alarms associated with that device or link.

**Step 3** Click on a device to view the device summary information (such as host name, IP address, and alarm summary). You can also launch the Device 360° view for additional device information.
Using Device 360° to View a Device’s Topology

You can use the Device 360° view to see the local, or $N$-hop, topology for a device. This lets you visualize where in the network the device is located and see its context within the overall network. This can be helpful if you are viewing the Alarm Browser and want to see more information about a specific device associated with an alarm. By launching the Device 360° view, you can see the local topology for that selected device.

**Step 1**
From the Device 360° view, click the **Topology** icon.

By default, Prime Infrastructure displays all devices within two hops of the device and the alarm status of all displayed devices and links.

**Step 2**
To modify the hop count, click the **Edit** icon and select a new value from the Hops pulldown menu.

**Related Topics**
- Topology Overview
- Determining What is Displayed in the Topology Map
- Getting More Information About Devices
- Getting More Information About Links
- Viewing Fault Information for Devices and Links
Changing the Topology Map Layout

You can specify how the devices and other network elements (such as labels, nodes, and the connections between them) are arranged in the topology map:

- Symmetrical (default)— Maintains the symmetry that is inherent in the topology. This ensures that adjacent nodes are closer to each other and prevents node overlapping.
- Circular— Arranges the network elements in a circular style highlighting the clusters inherent in the network topology.
- Hierarchical— Ensures that the dependencies on the relationships and flows between elements are maintained.
- Orthogonal— Creates a compact view of the topology using horizontal and vertical lines to represent the edge routing elements and links. This style minimizes edge route lengths, provides overlap-free label placement, and ensures that edge crossings can be clearly viewed.
- Incremental— Maintains the relative positions of specific elements while adjusting the positions of newly added elements. Use this layout to re-render nodes/links and to clean up overlaps.

When you choose a map layout, the elements align accordingly. You can also drag and drop elements to change the layout manually. After you have changed the layout, you can save it so that it will be preserved when you next open the Network Topology window. See Saving the Topology Map Layout.

---

Step 1 In the left sidebar, choose Maps > Network Topology.
Step 2 Select the required device group from the Groups pane on the left.
Step 3 Click the Layout icon in the topology toolbar and choose the required layout. The topology map display will be adjusted accordingly.

---

Related Topics
- Topology Overview
- Determining What is Displayed in the Topology Map
- Saving the Topology Map Layout

Saving the Topology Map Layout

Prime Infrastructurer retains your layout changes and your selections for the current browser session only. Therefore, after you have changed the topology map layout to suit your needs, it is highly recommended that you save the layout so that you do not have to manually rearrange the topology map each time.

Choose Layout > Save Current Layout from the Topology toolbar. You can reload the layout at any time by choosing Layout > Load Saved Layout.

Related Topics
- Topology Overview
- Saving the Topology Map as an Image File
Saving the Topology Map as an Image File

You can save the entire topology map or selected objects from the topology map as an image file. This will enable you to store copies of the topology map in a specific state which you can use as a point of reference in the future when multiple changes are made to the topology.

**Step 1** Choose Maps > Topology Maps > Network Topology or Datacenter Topology.

**Step 2** Select the required device group from the Groups pane on the left.

**Step 3** Make content and layout changes to the topology map as required.

**Step 4** Click the Save Image icon in the topology toolbar.

**Step 5** In the Save As Image dialog box, select the file type for the saved image.

**Step 6** Choose whether you want to save the entire topology or only the items currently selected in the topology map.

**Step 7** Choose a size setting for the image file.

**Step 8** Click Save. The image is saved in your local Temp folder and you return to the Network Topology screen.

**Related Topics**
- Topology Overview
- Determining What is Displayed in the Topology Map
- Changing the Topology Map Layout
- Saving the Topology Map Layout

Creating a Topology Dashlet

You can add a topology dashlet to the Overview dashboard to make it easier to view your physical network.

**Step 1** Choose Dashboard, then select the dashboard to which you want to add the topology dashlet.

**Step 2** Click the Settings icon, then choose Add Dashlet(s).

**Step 3** Click Add next to the Network Topology dashlet. You can drag and drop the topology dashlet to the desired location in the dashboard.

**Step 4** Edit the dashlet to enter a title and select the device group for which you want to display its topology.

**Related Topics**
- Topology Overview
- Changing the Topology Map Layout
- Saving the Topology Map Layout
Viewing vPc Summary

You can view the vPc summary.

---

**Step 1**  Choose *Maps > Topology Maps > Datacenter Topology.*

**Step 2**  Select the required device group from the Groups pane on the left and click on the information icon.

**Step 3**  Click *View VPC Summary.*

**Step 4**  Select the desired VPC from the table and click *View Inconsistency* to view the *VPC Configuration Consistency View.*
Using Wireless Maps

About Prime Infrastructure Site Maps

Prime Infrastructure site maps represent the geographical locations and physical structures where your organization maintains network assets and provides network services to its staff and guests.

Maps are a familiar way to visualize networks and services. Prime Infrastructure uses them to support many tasks, including:

- Displaying the physical locations of network devices, including wired routers, wireless access points and controllers, and client devices like laptops, tablets and mobile phones.
- Showing wireless network coverage, including “heatmap” displays of signal strength and quality, the locations of RF interferers, chokepoints, and so on.
- Diagramming the network topology.

Related Topics:
- Site Map Hierarchy
- Site Map Graphics
- Network Elements on Site Maps
- Preparing Image Files for Use with Prime Infrastructure Maps
- Working With Site Maps
- Creating Campus Maps
- Associating Endpoints with a Site

Site Map Hierarchy

Prime Infrastructure maps have a predetermined hierarchy:

- **Campus (or site) maps** are the highest level in the map hierarchy and represent a single business location or site. Typically, a campus map will consist of at least one building, with one or more floor areas, and any outside areas adjacent to the buildings that are served by your organization’s network devices.

- **Buildings** represent single structures within a campus, serving to organize related floor-area maps. You can add as many buildings as you like to a single campus map. A building can have one or more floor and outside areas associated with it, but can only be added to one campus map.
• **Floor areas** map the levels within a building interior, including working areas, cubicles, walled offices, wiring closets, and the like. Floor areas can only be added to building maps. You can add up to 100 floor areas and up to 100 basement levels to each building map you create.

• **Outside areas** map exterior locations served by your organization’s network (usually by its wireless network). Although they are typically associated with buildings, outside areas must be added directly to campus maps, at the same level as buildings. You can add as many outside areas to a campus map as you want.

Within these restrictions, you can create as many site maps as you need, arranged as you choose.

**Related Topics**

• Site Map Graphics
• Network Elements on Site Maps
• Wireless Coverage Areas, Inclusion/Exclusion Regions and Rail Lines on Maps
• Working With Site Maps

### Site Map Graphics

When you create your site maps, you can import them into aerial photos, map images, architectural layouts, and other graphics, specifying dimension and position information with the imported file. Prime Infrastructure scales imported map image files automatically, so that they fit the specified dimensions and position information. You can also specify contact data, civic address, and geographic longitude and latitude information for every campus and building.

**Related Topics**

• About Prime Infrastructure Site Maps
• Adding Floor Plans to a Standalone Building

### Network Elements on Site Maps

Once you have created your maps, you can assign network elements to them. You normally do this manually, selecting individual devices and assigning them to campuses, buildings, floors and outside areas as needed. In the case of wireless access points and access controllers, you can also add them to your maps automatically, using your organization’s AP/WAC naming hierarchy.

**Related Topics**

• About Prime Infrastructure Site Maps
• Working With Site Maps

### Wireless Coverage Areas, Inclusion/Exclusion Regions and Rail Lines on Maps

In addition to the basic site map hierarchy, Prime Infrastructure’s floor and outside area maps allow you to place the following features, which help you map wireless coverage more usefully:

• **Coverage Areas**: Any floor area or outside area defined as part of a building map is by default considered a wireless coverage area. Assuming that you have enabled
Inclusion regions define areas within a floor or outside area map where wireless coverage data, such as signal strength, will be either mapped (included) or ignored (excluded). Defining inclusion and exclusion regions can help you focus Prime Infrastructure processing to just those areas of the map where you want to manage your wireless coverage, and ignores others.

Exclusion regions define areas within a floor or outside area map where wireless coverage data, such as signal strength, will be ignored. Defining an exclusion region can help you focus Prime Infrastructure processing to just those areas of the map where you want to manage your wireless coverage, and ignores others.

Rail lines act as collection points for clients who are constantly roaming within a floor or outside area map. Wireless clients within a specified distance of a rail line will be shown as connected at the rail line, rather than at their actual location. This is handy for conveyor belts, internet cafes and other areas within a floor or outside area where many wireless clients cluster while remaining mobile.

Related Topics
- About Prime Infrastructure Site Maps
- Working With Site Maps

Preparing Image Files for Use with Prime Infrastructure Maps

As explained in the topic “Site Map Concepts”, you can import image files into any Prime Infrastructure campus, building, floor or outside area map. These image files will usually show:

- For campus/site maps: An aerial view or overhead diagram of the campus, showing all of the buildings on that campus or site.
- For floors, basements, and outside areas: Architectural layout diagrams.

Follow these guidelines when preparing map image files for import:

- Create the campus/site, floor, or outside area map image using any graphics application that saves to the raster image file formats PNG, JPG, JPEG or GIF.
- For floor and outside area maps only: You can also create the images as DXF or DWG CAD files, or as Qualcomm MET files. Prime Infrastructure will automatically convert these files to your choice of PNG, JPG, JPEG or GIF file formats.
- Always ensure that the dimensions of any campus/site map image are larger than the combined dimensions of all the buildings and outside areas you plan to add to the campus map.
- Your map image files can be of any size. Prime Infrastructure imports the original image to its database at full definition, but during display, automatically resizes them to fit the workspace.
- To make it easier to browse to select image files, copy them to a location in the file system of the client you use to access Prime Infrastructure before you import them. You can delete the image files from the client once they have been imported, as Prime Infrastructure makes them part of its image database.
- Gather the horizontal and vertical dimensions of the entire site, in feet or meters, so that you can specify these dimension during import.
- If you plan on entering campus, building, floor or outside area dimensions in meters, change the default map measurement unit to meters. For details, see “Changing Default Map Measurement Units” in Related Topics.
Preparation of Image Files for Use with Prime Infrastructure Maps

Related Topics

- About Prime Infrastructure Site Maps
- Troubleshooting Problems With CAD Image File Imports
- Changing Default Map Measurement Units

Troubleshooting Problems With CAD Image File Imports

Prime Infrastructure uses a native image-conversion library to convert CAD and MET vector files into raster format. You must select one of the following supported target raster formats during the CAD or MET file import: PNG, JPEG or (JPG), and GIF.

If for some reason Prime Infrastructure cannot load the native image-conversion library, it will display an “unable to convert the autocad file” error message. If you receive this error, make sure all the required dependencies are met for the native library, using the Linux `ldd` command. The following four DLLs must be present under the Prime Infrastructure installation directory `/webnms/rfdlls`: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems exist, you may need to install the required libraries and then restart the Prime Infrastructure server.

Floor and outside area map images imported from CAD files are enhanced for zooming and panning. Without zoom, the image clarity will be close to that of the original CAD file. But an imported CAD file can appear blurred during zoom. If you are having problems with blurred floor map images, first make sure all relevant parts of the image are clearly visible in the original CAD file. Then import the CAD file again, and choose PNG or GIF as the target conversion file format, instead of JPEG or JPG.

Large floor map images can take time to import. While the conversion is going on, not all of the image will be visible on the map. For example, if you have a high-resolution image (e.g., an image with a resolution of 180 megapixels and a file size of 60 MB), it may take two minutes or more for the imported image to appear on the map.

Related Topics

- Adding Floor Plans to a Standalone Building
- Administrator Guide restart link

Default Campus Maps

Prime Infrastructure comes with two default campus maps:

- **System Campus**: This is the default campus map. If you create any building, floor or outside area map, but do not create your own campus map, these subordinate maps are automatically created as children of the System Campus map.

- **Unassigned**: This is the default map for all network endpoints and hosts not assigned to any other map (including the System Campus).

Related Topics

- Adding Floor Plans to a Standalone Building
Disabling Next Generation Maps

Starting with version 2.0, Prime Infrastructure introduced Next Generation maps. These maps offer better performance and larger, more detailed map information than in previous versions of the product. Next Generation maps are enabled by default.

Step 1
Select Settings > My Preferences.

Step 2
Click the Use Next Generation Maps checkbox to unselect it.

Step 3
Click Save.

Related Topics
- Adding Floor Plans to a Standalone Building

Working With Site Maps

Choose Maps > Site Maps to display the Site Maps page. The Site Maps page contains the following information.

Site Maps page displays the number of 802.11a/n/ac, 802.11b/g/n radios available on the campus, building, floor, and the outdoor area. When the XOR radios on a floor or outdoor area change their modes to either serving or monitor and the band changes to 802.11a or 802.b, then the corresponding counts in the Site Map page changes.

- Name
- Type
- Incomplete
- Total APs
- a/n/ac Radios
- b/g/n Radios
- Radios with Critical Alarms
- Wireless Clients
- Status

You can choose to organize your site maps any way you wish. The workflow you will follow is similar:

1. Create a new campus map. Choose Maps > Site Maps, then from the Select a command list, choose New Campus.

2. Add a building to the campus map. Choose Maps > Site Maps, then from the Select a command list, choose New Building.

3. Add a floor to the building map. Choose Maps > Site Maps, then Select a command > New Floor Area > Go.

4. Add an outside area to the campus map. Choose Maps > Site Maps, then Select a command > New Outside Area > Go.

5. Use Map Editor to draw inclusion/exclusion regions and rail lines on your floor and outside areas. Choose Maps > Site Maps, select the floor or outside area, then choose Map Editor.
Creating Campus Maps

You must enter a unique name for the campus when you create it. Optionally, you can also:

- Specify an email, telephone, or other contact to be used for inquiries about the campus.
- Import a map image file into the campus map.
- Specify location information for the campus, including its mailing or street address and its longitude and latitude.

Once you have created a campus map, you will want to make it more useful by:

- Adding an image file showing an overview of the campus site.
- Add location information for the campus.
- Adding buildings to the campus.

For details on these tasks, see Related Topics.

Step 1  Choose Maps > Site Maps.
Step 2  Choose Select a command > New Campus > Go.
Step 3  On the Maps > New Campus page, enter the campus name and (optionally) a campus contact name.
Step 4  Click OK to add the campus map. Prime Infrastructure adds a hyperlink to the campus map in the Map Tree View.

Adding Image Files to Campus Maps

Importing a map image file into the background of a campus map helps you visualize and recognize the campus and its layout. When added with accurate location and dimension data, it also serves to locate your buildings and devices exactly.
To import a map image file into a previously created campus map, follow the steps below. Note that you can also import map image files when creating a campus map, by clicking Image File and specifying the campus map image file you want to import.

Before you begin, be sure you have prepared your campus map image as explained in “Preparing Image Files for User With Prime Infrastructure Maps”.

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the name of the campus map to which you want to import the image file. The Site Maps > Campus Name page appears.

**Step 3** From the Select a command list, choose Edit Campus/Site and click Go.

**Step 4** Next to Image File Name, click Choose File.

**Step 5** Browse to and choose the file containing the campus map image, then click Open.

**Step 6** Click Next.

**Step 7** Select the Maintain Aspect Ratio check box.

Selecting this setting prevents distortion when Prime Infrastructure resizes the imported map image.

**Step 8** Enter the campus site’s horizontal and vertical dimensions, in feet or meters.

**Step 9** Click OK. Prime Infrastructure displays the Campus/Site View page for the selected campus map, with the image file in the background.

**Related Topics**
- Adding Floor Plans to a Standalone Building
- Creating Campus Maps
- Adding Location Information to Campus Maps

### Adding Location Information to Campus Maps

Location information for a campus map includes the site’s mailing or street address and its geographical longitude and latitude. Adding this information is optional.

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the name of the desired campus map. The Site Maps > Campus Name page appears.

**Step 3** From the Select a command list, choose Edit Campus/Site and click Go.

**Step 4** Click Next.

**Step 5** Enter the site’s address and longitude/latitude information.

**Step 6** Click OK. Prime Infrastructure displays the Campus/Site View page for the selected campus map.

**Related Topics**
- Creating Campus Maps
- Adding Image Files to Campus Maps
Changing Default Map Measurement Units

The default unit of measurement for all Prime Infrastructure maps is feet. You can change this to meters.

**Step 1** Choose Maps > Site Maps.

**Step 2** From the Select a command list, choose Properties and click Go.

**Step 3** In Units of Measure, select the unit you want to use as the default unit (feet or meters) for all maps.

**Step 4** Click OK.

**Related Topics**
- Creating Campus Maps
- Adding Image Files to Campus Maps

Adding Buildings to Campus Maps

You can only add buildings to a campus map. If you do not add them to a campus map you created, Prime Infrastructure adds them to the default System Campus map automatically.

You must specify a unique name for the building. To create a useful building map, you will also want to specify:

- An email or telephone contact for the building.
- The number of floors and basements in the building.
  a. The building’s horizontal and vertical position on the campus map. The building’s horizontal position is the distance from the corner of the building rectangle to the left edge of the campus map. The vertical position is the distance from the corner of the building rectangle to the top edge of the campus map. You can enter these dimensions in feet or meters.
  b. The building’s approximate span — its horizontal and vertical “footprint”, or width and depth on the map — in feet or meters. The footprint you specify for the building should be equal to or larger than the span of any floors you plan to add to the same building.
- Location information for the building, including its mailing or street address and its geographical longitude and latitude.

Once you have created a building map, you will want to make it more useful by adding floor, basement and outdoor areas. For details on these tasks, see Related Topics.

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the name of the campus to which you want to add the building. The Site Maps > Campus Name page appears.

**Step 3** Choose Select a command > New Building > Go.

**Step 4** Complete the fields on the Campus Name > New Building page as needed. As you do so, be aware that:

- You must enter a name for the building. The name must be unique among the other building names you plan to add to the same campus map.
• Although you can specify the building’s exact position and span using the input fields, you can also specify its position and span using the mouse and keyboard:
  - **For Position changes:** Click and drag the blue bounding box in the upper left corner of the campus map to the desired position. As you drag, the values in the Horizontal Position and Vertical Position fields change to match your actions.
  - **For Span changes:** Ctrl+click and drag the blue bounding box to change the building’s span. As you drag, the values in the Horizontal Span and Vertical Span fields change to match your actions.

**Step 5**
When you are satisfied, click **Place** to put the building on the campus map. Prime Infrastructure creates a building rectangle scaled and positioned as you specified.

**Step 6**
Click **Save** to save the building. Prime Infrastructure places the building on the campus map, and the Site Maps Tree View displays a hyperlink for the building.

---

**Related Topics**
- Adding Floor Plans to a Standalone Building
- Creating Campus Maps
- Default Campus Maps
- Adding Location Information to Campus Maps
- Adding Image Files to Campus Maps
- Adding Floor Areas to Buildings

---

**Moving Buildings and Floors to Another Campus**

You can move any building from one campus to another without having to recreate it. Any floor areas you have created for the building will move with it. The destination campus must already exist before you attempt to move a building to it.

**Step 1**
Choose **Maps > Site Maps**.

**Step 2**
Click the selection box next to the name of each building you want to move to another campus.

**Step 3**
From the **Select a command** list, choose **Move Buildings** and click **Go**.

**Step 4**
In the **Target Campus/Site** list, choose the name of the campus map to which you want to move the selected buildings.

**Step 5**
Click **OK**.

On the Results page, click the **Edit Building** link to reposition the moved buildings on the new campus.

---

**Related Topics**
- Creating Campus Maps
- Adding Buildings to Campus Maps
- Adding Image Files to Campus Maps
Adding Floor Areas to Buildings

You can add floor and basement areas to any building you have added to a campus map. When doing so, bear in mind that:

- You can only add floor and basement areas to building maps.
- You can only add floor and basement areas up to the number of floors and basements you specified when you added the building to the campus map. If you made a mistake with these, you will need to edit the building map first.

When creating the floor area, you must specify at least the following:

- The floor area name. The floor name is distinct from the floor number, and must be unique not only to the building, but across all buildings on your campus maps.
- The floor number, which you can pick from a list.

To create a useful floor or basement area, you will also want to specify:

- An email or telephone contact for the floor or basement area.
- The RF model for the floor or basement (for example: “Drywall”). The model selected is used to calculate wireless signal strength, heat maps, and other wireless-related features for the floor or basement area.
- The floor-to-floor height, in meters or feet.
- The floor’s approximate span — its horizontal and vertical “footprint”, or width and depth on the map — in feet or meters. The footprint you specify for the floor should be equal to or less than the span of the building containing the floor.
- The floor’s horizontal and vertical position, or coordinates, within the campus. The floor’s horizontal position is the distance from the top left corner of the floor area rectangle to the left edge of the campus map. The floor’s vertical position is the distance from the top left corner of the floor area rectangle to the top edge of the campus map.
- The total floor area, in square meters or feet.

Step 1
Choose Maps > Site Maps.

Step 2
In the Maps Tree view, click the name of the campus containing the building to which you want to add a floor area.

Step 3
Click the building name to display the building map.

Step 4
Choose Select a command > New Floor Area > Go. The New Floor Area page appears.

Step 5
Complete the New Floor Area fields as needed.

Step 6
In the New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

d. Select the Image or CAD File check box.

e. Browse to and choose the desired floor or basement image or CAD filename, and click Open.

   If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

   We do not recommend a .JPEG (.JPG) format for an auto-cad conversion. Unless a JPEG is specifically required, use .PNG or .GIF format for higher quality images.

f. Click Next. At this point, if a CAD file was specified, a default image preview is generated and loaded.
Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, Prime Infrastructure displays the following error: “Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library.” For more information see the Prime Infrastructure online help or Prime Infrastructure documentation.

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

When you choose the floor or basement image filename, Prime Infrastructure displays the image in the building-sized grid.

g. If you have CAD file layers, you can select or deselect as many as you want and click Preview to view an updated image. Click Next when you are ready to proceed with the selected layers.

Enter the remaining parameters for the floor area.

h. Either leave the Maintain Aspect Ratio check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.

i. If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Use Ctrl-click to resize the image within the building-sized grid.

j. If desired, select the Launch Map Editor after floor creation check box to rescale the floor and draw walls.

k. Click OK to save this floor plan to the database. The floor is added to the Maps Tree View and the Maps > Site Maps list.

Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.

Step 7

Click any of the floor or basement images to view the floor plan or basement map.

You can zoom in or out to view the map at different sizes and you can add access points.

---

**Adding Image Files to Floor Areas**

To import a floor plan image file into a previously created floor area map, follow the steps below. Note that you can also import map image files when creating a floor area map, by clicking Image File and specifying the floor plan image file you want to import.

Before you begin, be sure you have prepared your floor area image as explained in “Preparing Image Files for User With Prime Infrastructure Maps”.

---

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the name of the campus map containing the building in which the floor area exists. The Site Maps > Campus Name page appears.

**Step 3** Click the name of the building containing the floor area to which you want to import the image file. The Site Maps > Building page appears.

**Step 4** Choose Select a command > Edit Floor > Go.
Adding Image Files to Floor Areas

Chapter 42      Using Wireless Maps

Step 5  Next to **Image File Name**, click **Choose File**.

Step 6  Browse to and choose the file containing the floor area image, then click **Open**.

Step 7  Click **Next**.

Step 8  Select the **Maintain Aspect Ratio** check box.

Selecting this setting prevents distortion when Prime Infrastructure resizes the imported image.

Step 9  Enter the floor area’s horizontal and vertical dimensions, in feet or meters.

Step 10 Click **OK**. Prime Infrastructure displays the View page for the selected floor area, with the image file in the background.

---

**Related Topics**

- Adding Floor Plans to a Standalone Building
- Creating Campus Maps
- Adding Location Information to Campus Maps

---

**Adding Floor Plans to a Standalone Building**

After you have added a standalone building to the Prime Infrastructure database, you can add individual floor plan maps to the building.

To add floor plans to a standalone building, follow these steps:

---

Step 1  Save your floor plan maps in .PNG, .JPG, or .GIF format.

The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Step 2  Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.

If there are problems converting the auto-cad file, an error message is displayed. Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the Prime Infrastructure displays an “unable to convert the auto-cad file” message. If you receive this error, make sure all the required dependencies are met for the native library.

To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occur, you might need to install the required libraries and restart Prime Infrastructure.

Step 3  Choose **Maps > Site Maps**.

Step 4  From the Maps Tree View or the Maps > Site Maps left sidebar menu, choose the desired building to display the Building View page.

The building view displays the number of 802.11a and 802.11b radios in each floor along with the clients attached to each band (802.11a and 802.11b). When the XOR radios in these floors change their band, then the corresponding client count changes.

- Floor Area
- Floor Index
- Contact
Chapter 42  Using Wireless Maps

Adding Image Files to Floor Areas

- Status
- a/n/ac Clients
- Wired Clients
- Total APs
- a/n/ac Radios
- b/g/n Radios
- Radios with Critical Alarms
- b/g/n Clients

**Step 5**  From the Select a command drop-down list, choose New Floor Area.

**Step 6**  Click Go.

**Step 7**  In the New Floor Area page, add the following information:
- Enter the floor area and contact names.
- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet.
- Select the Image or CAD File check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click Open.

---

**Note**  If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

---

**Tip**  A JPEG (JPG) format is not recommended for an AutoCAD conversion. Unless a JPEG is specifically required, use a PNG or GIF format for higher quality images.

**Step 8**  Click Next. At this point, if a CAD file was specified, a default image preview is generated and loaded.

---

**Note**  Prime Infrastructure uses a native image conversion library to convert AutoCAD files into raster formats like PNG. When there are issues loading the native library, Prime Infrastructure displays the following error: “Unable to convert the AutoCAD file. Reason: Error while loading the AutoCAD image conversion library. For more information, see the Prime Infrastructure online help or Prime Infrastructure documentation.”

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

When you choose the floor or basement image filename, Prime Infrastructure displays the image in the building-sized grid.

The maps can be any size because Prime Infrastructure automatically resizes the maps to fit the workspace.

---

**Note**  The map must be saved in PNG, JPG, JPEG, or GIF format.
If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

**Step 9** Enter the remaining parameters for the floor area.

- Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.
  
  The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.
- If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

**Tip**  
Use **Ctrl-click** to resize the image within the building-sized grid.

- Adjust the floor characteristics with the Prime Infrastructure map editor by selecting the check box next to **Launch Map Editor**. See the **Using the Map Editor** for more information regarding the map editor feature.

**Step 10** Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Maps > Site Maps list.

**Step 11** Click any of the floor or basement images to view the floor plan or basement map.

You can zoom in or out to view the map at different sizes and you can add access points.

### Getting AP Details from 360° View

The 360° view provides the details of the selected access point on the floor view. To launch the 360° view of the access point, click the access point icon on the floor map.
You can modify the appearance of the floor map by selecting or unselecting various floor settings check boxes. The selected floor settings appears in the map image.

The Floor Settings options include the following:

- Access Points
- AP Heatmaps
- AP Mesh Info
- Clients
- 802.11 Tags
- Rogue APs
- Rogue Adhocs
- Rogue Clients
- Coverage Areas

### Table 42-1 AP 360° View Features

<table>
<thead>
<tr>
<th>Device 360° View Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action drop-down list</td>
<td>Choose one of the following options from the Action drop-down list.</td>
</tr>
<tr>
<td></td>
<td>- Monitor Access Point—Launches the Access Point Details page. See Monitoring Access Point Details for more information.</td>
</tr>
<tr>
<td></td>
<td>- Configure Access Point—See Configuring Access Point Details for more information.</td>
</tr>
<tr>
<td></td>
<td>- Associated Client—Launches the Clients and Users page. See Viewing Clients and Users for more information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>802.11a/n/ac</th>
<th>Lists these information:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Radio Interface Summary</td>
</tr>
<tr>
<td></td>
<td>- Rx Neighbors details</td>
</tr>
<tr>
<td></td>
<td>- Interferers details for 802.11a/n/ac radio.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>XOR radio</th>
<th>Lists these information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any of these tabs are displayed based on the band selection:</td>
<td>- Radio Interface Summary</td>
</tr>
<tr>
<td></td>
<td>- Rx Neighbors details</td>
</tr>
<tr>
<td></td>
<td>- Interferers details for XOR radio.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarms</th>
<th>Lists alarms on the device, including the alarm status, time stamp, and category.</th>
</tr>
</thead>
</table>

| Ethernet Interfaces      | Lists switch Ethernet interface details such as interface name, link speed, operation status, admin status, and duplex. |

### Configuring Floor Settings

You can modify the appearance of the floor map by selecting or unselecting various floor settings check boxes. The selected floor settings appears in the map image.
• Location Regions
• Rails
• Markers
• Chokepoints
• Wi-Fi TDOA Receivers
• Interferers

Use the blue arrows to access floor setting filters for access points, access point heatmaps, clients, 802.11 tags, rogue access points, rogue adhocs, and rogue clients. When filtering options are selected, click **OK**.

Use the Show MSE data within last drop-down list to choose the timeframe for mobility services engine data. Choose to view mobility services engine data from a range including the past two minutes up to the past 24 hours. This option only appears if a mobility services engine is present on Prime Infrastructure.

Click **Save Settings** to make the current view and filter settings your new default for all maps.

### Defining Inclusion and Exclusion Regions on a Floor

To further refine location calculations on a floor, you can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion areas).

For example, you might want to exclude areas such as an atrium or stairwell within a building but include a work area (such as cubicles, labs, or manufacturing floors).

**Note**

If the MSE to which the floor is synchronized is running the Aeroscout tag engine, then inclusion and exclusion regions are not calculated for tags.

### Viewing Floor Component Details

To view details regarding the components displayed on the Floor View, hover your mouse cursor over the applicable icon. A dialog box containing detailed information is displayed. Table 42-2 displays the floor map icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Access point icon" /></td>
<td>Access point icon. The color of the circle indicates the alarm status of the Cisco Radios. <strong>Note</strong> Each access point contains two Cisco Radios. When a single protocol is selected in the Access Point filter page, the entire icon represents this radio. If both protocols are selected, the top half of the icon represents the state of the 802.11a/n radio and the bottom half represents the state of the 802.11b/g/n radio. <strong>Note</strong> If a Cisco Radio is disabled, a small “x” appears in the middle of the icon. <strong>Note</strong> Monitor mode access points are shown with a gray label to distinguish these from other access points.</td>
</tr>
<tr>
<td><img src="image" alt="AP heatmaps icon" /></td>
<td>AP heatmaps icon.</td>
</tr>
<tr>
<td><img src="image" alt="Client icon" /></td>
<td>Client icon. Hover your mouse cursor over the icon to view client details.</td>
</tr>
</tbody>
</table>
### Table 42-2  Floor Map Icons (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Tag" /></td>
<td>Tag icon. Hover your mouse cursor over the icon to view tag details.</td>
</tr>
<tr>
<td><img src="image" alt="Rogue Access Point" /></td>
<td>Rogue access point icon. The color of the icon indicates the type of rogue access point. For example, red indicates a malicious rogue access point and blue indicates an unknown type. Hover your mouse cursor over the icon to view rogue access point details.</td>
</tr>
<tr>
<td><img src="image" alt="Rogue Adhoc" /></td>
<td>Rogue adhoc icon. Hover your mouse cursor over the icon to view rogue adhoc details.</td>
</tr>
<tr>
<td><img src="image" alt="Rogue Client" /></td>
<td>Rogue client icon. Hover your mouse cursor over the icon to view rogue client details.</td>
</tr>
<tr>
<td><img src="image" alt="Coverage" /></td>
<td>Coverage icon.</td>
</tr>
<tr>
<td><img src="image" alt="Location Regions" /></td>
<td>Location regions icon.</td>
</tr>
<tr>
<td><img src="image" alt="Rails" /></td>
<td>Rails icon.</td>
</tr>
<tr>
<td><img src="image" alt="Marker" /></td>
<td>Marker icon.</td>
</tr>
<tr>
<td><img src="image" alt="Chokepoint" /></td>
<td>Chokepoint icon.</td>
</tr>
<tr>
<td><img src="image" alt="Wi-Fi TDOA Receiver" /></td>
<td>Wi-Fi TDOA receiver icon.</td>
</tr>
<tr>
<td><img src="image" alt="Interferer Device" /></td>
<td>Interferer device icon.</td>
</tr>
<tr>
<td><img src="image" alt="Indicates Guest" /></td>
<td>Indicates a guest client that is configured through web auth WLAN on Prime Infrastructure. <strong>Note</strong> If you create a Guest WLAN on controller and assign that controller to MSE, only then the guests from that controller will show as guest icons.</td>
</tr>
</tbody>
</table>

### Cisco 1000 Series Lightweight Access Point Icons

The icons indicate the present status of an access point. The circular part of the icon can be split in half horizontally. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer.

**Note** When the icon is representing 802.11a/n and 802.11b/n, the top half displays the 802.11a/n status, and the bottom half displays the 802.11b/g/n status. When the icon is representing only 802.11b/g/n, the whole icon displays the 802.11b/g/n status. The triangle indicates the more severe color.
Table 42-3 shows the icons used in the Prime Infrastructure user interface Map displays.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green Icon" /></td>
<td>The green icon indicates an access point (AP) with no faults. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.</td>
</tr>
</tbody>
</table>
| ![Yellow Icon](image) | The yellow icon indicates an access point with a minor fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio.  
**Note** A flashing yellow icon indicates that there has been an 802.11a or 802.11b/g interference, noise, coverage, or load profile failure. A flashing yellow icon indicates that there have been 802.11a and 802.11b/g profile failures. |
| ![Red Icon](image) | The red icon indicates an access point (AP) with a major or critical fault. The top half of the circle represents the optional 802.11a Cisco Radio. The bottom half of the circle represents the state of the 802.11b/g Cisco Radio. |
| ![Dimmed Icon](image) | The dimmed icon with a question mark in the middle represents an unreachable access point. It is gray because its status cannot be determined. |
| ![Dimmed Icon](image) | The dimmed icon with no question mark in the middle represents an unassociated access point. |
| ![Red X Icon](image) | The icon with a red “x” in the center of the circle represents an access point that has been administratively disabled. |
| ![Green and Yellow Icon](image) | The icon with the top half green and the lower half yellow indicates that the optional 802.11a Cisco Radio (top) has no faults, and the 802.11b/g Cisco Radio (bottom) has a minor fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer. |
| ![Green and Red Icon](image) | The icon with the top half green and the lower half red indicates that the optional 802.11a Cisco Radio (top) is operational with no faults, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer. |
| ![Yellow and Red Icon](image) | The icon with the top half yellow and the lower half red indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) has a major or critical fault. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer. |
| ![Yellow and Green Icon](image) | The icon with the top half yellow and the lower half green indicates that the optional 802.11a Cisco Radio (top) has a minor fault, and the 802.11b/g Cisco Radio (bottom) is operational with no faults. The more severe of the two Cisco Radio colors determines the color of the large triangular pointer. |
Each of the access point icons includes a small black arrow that indicates the direction in which the internal Side A antenna points.

Table 42-4 shows some arrow examples used in the Prime Infrastructure user interface map displays.

<table>
<thead>
<tr>
<th>Arrow Examples</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Zero degrees, or to the right on the map.</td>
</tr>
<tr>
<td></td>
<td>45 degrees, or to the lower right on the map.</td>
</tr>
</tbody>
</table>
Filtering Access Point Floor Settings

If you enable the access point floor setting and then click the blue arrow to the right of the floor settings, the Access Point Filter dialog box appears with filtering options.

Access point filtering options include the following:

- **Show**—Select this radio button to display the radio status or the access point status.

  **Note** Because the access point icon color is based on the access point status, the icon color might vary depending on the status selected. The default on floor maps is radio status.

- **Protocol**—From the drop-down list, choose which radio types to display (802.11a/n/ac, 802.11b/g/n, or both).

  The displayed heatmaps correspond to the selected radio type(s).

- **Display**—From the drop-down list, choose what identifying information is displayed for the access points on the map image.
  - **Channels**—Displays the Cisco Radio channel number or Unavailable (if the access point is not connected).
  - **TX Power Level**—Displays the current Cisco Radio transmit power level (with 1 being high) or Unavailable (if the access point is not connected).

  The power levels differ depending on the type of access point. The 1000 series access points accept a value between 1 and 5, the 1230 access points accept a value between 1 and 7, and the 1240 and 1100 series access points accept a value between 1 and 8.

  **Table 42-5** lists the transmit power level numbers and their corresponding power setting.

### Table 42-5  Transmit Power Level Values

<table>
<thead>
<tr>
<th>Transmit Power Level Number</th>
<th>Power Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Maximum power allowed per country code setting</td>
</tr>
<tr>
<td>2</td>
<td>50% power</td>
</tr>
<tr>
<td>3</td>
<td>25% power</td>
</tr>
<tr>
<td>4</td>
<td>12.5 to 6.25% power</td>
</tr>
<tr>
<td>5</td>
<td>6.25 to 0.195% power</td>
</tr>
</tbody>
</table>
Note: The power levels are defined by the country code setting and are regulated by country. See the following URL for more information: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

- Channel and Tx Power—Displays both the channel and transmit power level (or Unavailable if the access point is not connected).
- Coverage Holes—Displays a percentage of clients whose signal has become weaker until the client lost its connection, Unavailable for unconnected access points, or MonitorOnly for access points in monitor-only mode.

Note: Coverage holes are areas in which clients cannot receive a signal from the wireless network. When you deploy a wireless network, you must consider the cost of the initial network deployment and the percentage of coverage hole areas. A reasonable coverage hole criterion for launch is between 2 and 10 percent. This means that between two and ten test locations out of 100 random test locations might receive marginal service. After launch, Cisco Unified Wireless Network Solution Radio Resource Management (RRM) identifies these coverage hole areas and reports them to the IT manager, who can fill holes based on user demand.

- MAC Addresses—Displays the MAC address of the access point, whether or not the access point is associated to a controller.
- Names—Displays the access point name. This is the default value.
- Controller IP—Displays the IP address of the controller to which the access point is associated or Not Associated for disassociated access points.
- Utilization—Displays the percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays Unavailable for disassociated access points and MonitorOnly for access points in monitor-only mode.
- Profiles—Displays the load, noise, interference, and coverage components of the corresponding operator-defined thresholds. Displays Okay for thresholds not exceeded, Issue for exceeded thresholds, or Unavailable for unconnected access points.

Use the Profile Type drop-down list to choose Load, Noise, Interference, or Coverage.
- CleanAir Status—Displays the CleanAir status of the access point and whether or not CleanAir is enabled on the access point.
- Average Air Quality—Displays the average air quality on this access point. The details include the band and the average air quality.
- Minimum Air Quality—Displays the minimum air quality on this access point. The details include the band and the minimum air quality.
- Average and Minimum Air Quality—Displays the average and minimum air quality on this access point. The details include the band, average air quality, and minimum air quality.
- Associated Clients—Displays the number of associated clients, Unavailable for unconnected access points or MonitorOnly for access points in monitor-only mode.
- Bridge Group Names
- Dual-Band Radios—Identifies and labels the XOR dual band radios on the Cisco Aironet 2800 and 3800 Series Access Points.
- RSSI Cutoff—From the drop-down list, choose the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBm.
- Show Detected Interferers—Select the check box to display all interferers detected by the access point.
- Max. Interferers/label—Choose the maximum number of interferers to be displayed per label from the drop-down list.

Click **OK** when all applicable filtering criteria are selected.

**Filtering Access Point Heatmap Floor Settings**

An RF heatmap is a graphical representation of RF wireless data where the values taken by variables are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, Antenna Orientation, and AP transmit power.

If you enable the Access Point Heatmap floor setting and click the blue arrow to the right of the Floor Settings, the Contributing APs dialog appears with heatmap filtering options.

Prime Infrastructure introduces dynamic heatmaps. When dynamic heatmaps are enabled, the Prime Infrastructure recomputes the heatmaps to represent changed RSSI values.

Access point heatmap filtering options include the following:

- **Heatmap Type**
  - Coverage—If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points.
  - Air Quality—Not applicable for XOR Monitor mode radios. If you choose Air Quality, you can further filter the heat map type for access points with average air quality or minimum air quality. Select the appropriate radio button. It displays heatmaps for radios operating in client serving mode. Cisco Aironet 2800 and 3800 Series APs operate with Fixed-A band and XOR 2.4 GHz or XOR 5.4 GHz mode radios.
  - IDS—Available only for radios operating in monitor mode. IDS heatmap option is displayed only if there is at least one AP in the floor in the monitor mode or at least one XOR radio in the monitor mode.

  **Note** Only APs in Local, FlexConnect, or Bridge mode can contribute to the Coverage and Air Quality Heatmap.

  - Show only XOR—Displays heatmaps only for the XOR radios. With this you can differentiate between the heatmaps for fixed and dual band radios.
  - Total APs—Displays the number of access points positioned on the map.
  - Select the access point check box(es) to determine which heatmaps are displayed on the image map.

Click **OK** when all applicable filtering criteria are selected.

**Filtering AP Mesh Info Floor Settings**

The AP Mesh Info check box only appears when bridging access points are added to the floor.

When this check box is selected, Prime Infrastructure initiates a contact with the controllers and displays information about bridging access points. The following information is displayed:

  - Link between the child and the parent access point.
An arrow that indicates the direction from the child to parent access point.

A color-coded link that indicates the signal-to-noise ratio (SNR). A green link represents a high SNR (above 25 dB), an amber link represents an acceptable SNR (20-25 dB), and a red link represents a very low SNR (below 20 dB).

If you enable the AP Mesh Info floor setting and click the blue arrow to the right of the floor settings, the Mesh Parent-Child Hierarchical View page appears with mesh filtering options.

You can update the map view by choosing the access points you want to see on the map. From the Quick Selections drop-down list, choose to select only root access point, various hops between the first and the fourth, or select all access points.

**Note**

For a child access point to be visible, its parent must also be selected.

Click **OK** when all applicable filtering criteria are selected.

### Filtering Client Floor Settings

The Clients option only appears if a mobility server is added in Prime Infrastructure.

If you enable the Clients floor setting and click the blue arrow to the right, the Client Filter dialog box appears.

Client filtering options include the following:

- **Show All Clients**—Select the check box to display all clients on the map.
- **Small Icons**—Select the check box to display icons for each client on the map.

**Note**

If you select the **Show All Clients** check box and **Small Icons** check box, all other drop-down list options are dimmed.

If you unselect the **Small Icons** check box, you can choose if you want the label to display the MAC address, IP address, username, asset name, asset group, or asset category.

If you unselect the **Show All Clients** check box, you can specify how you want the clients filtered and enter a particular SSID.

- **Display**—Choose the client identifier (IP address, username, MAC address, asset name, asset group, or asset category) to display on the map.
- **Filter By**—Choose the parameter by which you want to filter the clients (IP address, username, MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.

If there are multiple IPv6 addresses for a client, then you can specify any one IP address to uniquely identify the client.

- **SSID**—Enter the client SSID in the available text box.
- **Protocol**—Choose All, 802.11a/n, or 802.11b/g/n from the drop-down list.
  - **All**—Displays all the access points in the area.
  - **802.11a/n**—Displays a colored overlay depicting the coverage patterns for the clients with 802.11a/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm).
Chapter 42      Using Wireless Maps

Adding Image Files to Floor Areas

- 802.11b/g/n—Displays a colored overlay depicting the coverage patterns for the clients with 802.11b/g/n radios. The colors show the received signal strength from red (–35 dBm) through dark blue (–85 dBm). This is the default value.

- State—Choose All, Idle, Authenticated, Probing, or Associated from the drop-down list.

Click OK when all applicable filtering criteria are selected.

Filtering 802.11 Tag Floor Settings

If you enable the 802.11 Tags floor setting and then click the blue arrow to the right, the Tag Filter dialog appears.

Tag filtering options include the following:

- Show All Tags—Select the check box to display all tags on the map.
- Small Icons—Select the check box to display icons for each tag on the map.

**Note**

If you select the Show All Tags check box and Small Icons check box, all other drop-down list options are dimmed.

If you unselect the Small Icons check box, you can choose if you want the label to display MAC address, asset name, asset group, or asset category.

If you unselect the Show All Tags check box, you can specify how you want the tags filtered.

- Display—Choose the tag identifier (MAC address, asset name, asset group, or asset category) to display on the map.
- Filter By—Choose the parameter by which you want to filter the clients (MAC address, asset name, asset group, asset category, or controller). Once selected, type the specific device in the text box.

Click OK when all applicable filtering criteria are selected.

Filtering Rogue AP Floor Settings

If you enable the Rogue APs floor setting and then click the blue arrow to the right, the Rogue AP filter dialog box appears.

Rogue AP filtering options include the following:

- Show All Rogue APs—Select the check box to display all rogue access points on the map.
- Small Icons—Select the check box to display icons for each rogue access point on the map.

**Note**

If you select the Show All Rogue APs check box and Small Icons check box, all other drop-down list options are dimmed.

If you unselect the Show All Rogue APs check box, you can specify how you want the rogue access points filtered.

- MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.
- State—Use the drop-down list to choose from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.
- On Network—Use the drop-down list to specify whether or not you want to display rogue access points on the network.

Click OK when all applicable filtering criteria are selected.

Filtering Rogue Adhoc Floor Settings

If you enable the Rogue Adhocs floor setting and then click the blue arrow to the right, the Rogue Adhoc filter dialog appears.

Rogue Adhoc filtering options include the following:
- Show All Rogue Adhocs—Select the check box to display all rogue adhoc on the map.
- Small Icons—Select the check box to display icons for each rogue adhoc on the map.

**Note**

If you select the **Show All Rogue Adhocs** check box and **Small Icons** check box, all other drop-down list options are dimmed.

If you unselect the **Show All Rogue Adhocs** check box, you can specify how you want the rogue adhocs filtered.

- MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.
- State—Use the drop-down list to select from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.
- On Network—Use the drop-down list to specify whether or not you want to display rogue adhocs on the network.

Click OK when all applicable filtering criteria are selected.

Filtering Rogue Client Floor Settings

If you enable the Rogue Clients floor setting and then click the blue arrow to the right, the Rogue Clients filter dialog appears.

Rogue Clients filtering options include the following:
- Show All Rogue Clients—Select the check box to display all rogue clients on the map.
- Small Icons—Select the check box to display icons for each rogue client on the map.

If you select the **Show All Rogue Clients** check box and **Small Icons** check box, all other drop-down list options are dimmed. If you unselect the **Show All Rogue Clients** check box, you can specify how you want the rogue clients filtered.

- Assoc. Rogue AP MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.
- State—Use the drop-down list to choose from Alert, Contained, Threat, or Unknown contained states.

Click OK when all applicable filtering criteria are selected.

Filtering Interferer Settings

If you enable Interferer floor setting and then click the blue arrow to the right, the Interferers filter dialog box appears.

Interferer filtering options include the following:
- Show active interferers only—Select the check box to display all active interferers.
- Small Icons—Select the check box to display icons for each interferer on the map.
- Show Zone of Impact—Displays the approximate interference impact area. The opacity of the circle denotes its severity. A solid red circle represents a very strong interferer that likely disrupts Wi-Fi communications, a light pink circle represents a weak interferer.
- Click **OK** when all applicable filtering criteria are selected.

### Import Map and AP Location Data

When converting from autonomous to lightweight access points and from the WLSE to Prime Infrastructure, one of the conversion steps is to manually reenter the access point-related information into Prime Infrastructure. To speed up this process, you can export the information about access points from the WLSE and import it into Prime Infrastructure.

**Note**

Prime Infrastructure expects a .tar file and checks for a .tar extension before importing the file. If the file you are trying to import is not a .tar file, Prime Infrastructure displays an error message and prompts you to import a different file.

**Note**

For more information on the WLSE data export functionality (WLSE Version 2.15), see the following URL:


To map properties and import a tar file containing WLSE data using the Prime Infrastructure web interface, follow these steps:

1. **Step 1** Choose Maps > Site Maps.
2. **Step 2** From the **Select a command** drop-down list, choose Import Maps, and click **Go**.
3. **Step 3** Choose the **WLSE Map and AP Location Data** option, and click **Next**.
4. **Step 4** In the Import WLSE Map and AP Location Data page, click **Browse** to select the file to import.
5. **Step 5** Find and select the .tar file to import and click **Open**.
   Prime Infrastructure displays the name of the file in the Import From text box.
6. **Step 6** Click **Import**.
   Prime Infrastructure uploads the file and temporarily saves it into a local directory while it is being processed. If the file contains data that cannot be processed, Prime Infrastructure prompts you to correct the problem and retry. Once the file has been loaded, Prime Infrastructure displays a report of what is added to Prime Infrastructure. The report also specifies what cannot be added and why.
   If some of the data to be imported already exists, Prime Infrastructure either uses the existing data in the case of campuses or overwrites the existing data using the imported data in the cases of buildings and floors.
Note

If there are duplicate names between a WLSE site and building combination and Prime Infrastructure campus (or top-level building) and building combination, Prime Infrastructure displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

Step 7

Click Import to import the WLSE data.
Prime Infrastructure displays a report indicating what was imported.

Step 8

Choose Monitor > Site Maps to view the imported data.

Monitoring Floor Areas

The floor area is the area of each floor of the building measured to the outer surface of the outer walls including the area of lobbies, cellars, elevator shafts, and in multi-dwelling buildings, all the common spaces.

- Panning and Zooming with Next Generation Maps, page 42-xxvii
- Adding Access Points to a Floor Area, page 42-xxviii
- Placing Access Points, page 42-xxx

Panning and Zooming with Next Generation Maps

Panning
To move the map, click and hold the left mouse button and drag the map to a new place.

You can also move the map North, South, East or West using the pan arrows. These can be found in the top left hand corner of the map (see Figure 42-1).

Figure 42-1  Panning Control

Note

You can also perform the panning operations using the arrow keys on a keyboard.

Zooming in and out - changing the scale
The zooming levels depend upon the resolution of an image. A high resolution image may provide more zoom levels. Each zoom level is made of a different style map shown at different scales, each one showing more or less detail. Some maps will be of the same style, but at a smaller or larger scale.

To see a map with more detail you need to zoom in. You can do this using the zoom bar on the left hand side of the map (see Figure 42-2). Click the + sign on the top of the zoom bar. To center and zoom in on a location, double click the location. To see a map with less detail you need to zoom out. To do this, click the - sign on the bottom of the zoom bar.
You can perform zooming operations using mouse or keyboard. With keyboard, click the + or - signs to zoom in or zoom out. With mouse, use the mouse scroll wheel to zoom in or zoom out or double click to zoom in.

**Floor View Navigation**

The Floor View navigation pane provides access to multiple map functions. This navigation pane includes the following functionality:

- **Zoom In/Zoom Out**—See the “Panning and Zooming with Next Generation Maps” section.
- **Map Size**—See the “Panning and Zooming with Next Generation Maps” section.
- **Show Grid**—Click to show or hide the grid that displays distance in feet on the map.
- **RSSI Legend**—Hover your mouse cursor over the RSSI Legend icon to display the RSSI color scheme (ranging from red/-35 dBm to dark blue/-90 dBm).
- **Add Access Points**—Click to open the Add Access Points page. For more information, see the “Adding Access Points to a Floor Area” section.
- **Remove Access Points**—Click to open the Remove Access Points page. Select the access points that you want to remove and click OK.
- **Position APs**—Click to open the Position Access Points page.
- **Add Chokepoints**—Click to open the Add Chokepoints page. For more information, see the Cisco Context-Aware Services Configuration Guide.
- **Add WiFi TDOA Receivers**—Click to open the Add Wi-Fi TDOA Receivers page. For more information, see the Cisco Context-Aware Services Configuration Guide.
- **Auto Refresh**—From the drop-down list, choose the length of time between each system refresh.
- **Refresh from Network**—Click to initiate an immediate refresh of the current data.
- **Planning Mode**—Click to open the Planning Mode window. For more information, see the “Using Planning Mode” section for more information.
- **Map Editor**—Click to open the Map Editor.

**Adding Access Points to a Floor Area**

After you add the .PNG, .JPG, .JPEG, or .GIF format floor plan and outdoor area maps to the Prime Infrastructure database, you can position lightweight access point icons on the maps to show where they are installed in the buildings. To add access points to a floor area and outdoor area, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** From the Maps Tree View or the Maps > Site Maps left sidebar menu, select the applicable floor to open the Floor View page.
Step 3 From the **Select a command** drop-down list, choose **Add Access Points**, and click **Go**.

Step 4 In the **Add Access Points** page, select the check boxes of the access points that you want to add to the floor area.

To search for access points, enter AP name or MAC address (Ethernet/Radio)/IP in the Search AP [Name/Mac Address (Ethernet/Radio)/IP] text box, and then click **Search**. The search is case-insensitive.

Only access points that are not yet assigned to any floor or outdoor area appear in the list. Select the check box at the top of the list to select all access points.

Step 5 When all of the applicable access points are selected, click **OK** located at the bottom of the access point list.

The Position APs page appears. The position AP screen is displayed when access points are moved within the floor view.

Each access point you have chosen to add to the floor map is represented by a gray circle (differentiated by access point name or MAC address) and is lined up in the upper left part of the floor map.

Step 6 Click and drag each access point to the appropriate location. Access points turn blue when selected.

When you drag an access point on the map, its horizontal and vertical position appears in the Horizontal and Vertical text boxes.

The small black arrow at the side of each access point represents Side A of each access point, and each access point arrow must correspond with the direction in which the access points were installed. Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio. To adjust the directional arrow, choose the appropriate orientation from the Antenna Angle drop-down list.

When selected, the access point details are displayed on the left side of the page. Selected AP Details include the following:

- **AP Model**—Indicates the model type of the selected access point.
- **MAC Address**—Displays the MAC address.
- **Protocol**—Choose the protocol for this access point from the drop-down list: 802.11a/n/ac, 802.11b/g/n (for Hyper Location APs), or 802.11a/b/g/n.
- **Horiz**—Enter the horizontal span of the map in feet.
- **Vert**—Enter the vertical span of the map in feet.
- **AP Height**—Enter the height of the access point.
- **Antenna**—Choose the appropriate antenna type for this access point from the drop-down list.
- **Antenna/AP Image**—The antenna image reflects the antenna selected from the Antenna drop-down list. Click the arrow at the top right of the antenna image to expand the image size.
- **Antenna Orientation**—Depending on the antenna type, enter the Azimuth and the Elevation orientations in degrees.
- **Azimuth**—This option does not appear for Omnidirectional antennas because their pattern is non-directional in azimuth.

**Note** For internal antennas, the same elevation angle applies to both radios.

The antenna angle is relative to the map X axis. Because the origin of the X (horizontal) and Y (vertical) axes is in the upper left corner of the map, 0 degrees points side A of the access point to the right, 90 degrees points side A down, 180 degrees points side A to the left, and so on.
The antenna elevation is used to move the antenna vertically, up or down, to a maximum of 90 degrees.

**Note** Make sure each access point is in the correct location on the map and has the correct antenna orientation. Accurate access point positioning is critical when you use the maps to find coverage holes and rogue access points.


**Step 7** When you are finished placing and adjusting each access point, click **Save**.

**Note** Clicking Save causes the antenna gain on the access point to correspond to the selected antenna. This might cause the radio to reset.

Prime Infrastructure computes the RF prediction for the entire map. These RF predictions are popularly known as *heat maps* because they show the relative intensity of the RF signals on the coverage area map. This display is only an approximation of the actual RF signal intensity because it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

**Note** Antenna gain settings have no effect on heatmaps and location calculations. Antenna gain is implicitly associated to the antenna name. Because of this, the following apply:
- If an antenna is used and marked as “Other” in Prime Infrastructure, it is ignored for all heatmap and location calculations;
- If an antenna is used and marked as a Cisco antenna in Prime Infrastructure, that antenna gain setting (internal value on Prime Infrastructure) is used no matter what gain is set on the controller.

See the “Placing Access Points” section on page 42-xxx for more information on placing access points on a map.

You can change the position of access points by importing or exporting a file. See the “Positioning Wi-Fi TDOA Receivers” section on page 42-xlvi for more information.

### Placing Access Points

To determine the best location of all devices in the wireless LAN coverage areas, you need to consider the access point density and location.

Ensure that no fewer than 3 access points, and preferably 4 or 5, provide coverage to every area where device location is required. The more access points that detect a device, the better. This high level guideline translates into the following best practices, ordered by priority:

1. Most importantly, access points should surround the desired location.
2. One access point should be placed roughly every 50 to 70 linear feet (about 17 to 20 meters). This translates into one access point every 2,500 to 5000 square feet (about 230 to 450 square meters).
Chapter 42  Using Wireless Maps

Using the Automatic Hierarchy to Create Maps

Automatic Hierarchy Creation is a way for you to quickly create maps and assign access points to maps in Prime Infrastructure. You can use Automatic Hierarchy Creation to create maps, once you have added wireless LAN controllers to Prime Infrastructure and named your access points. Also, you can use it after adding access points to your network to assign access points to maps in Prime Infrastructure.

Table 42-6 describes the orientation of the access points.

<table>
<thead>
<tr>
<th>Access Point</th>
<th>Antenna Orientation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1140 mounted on the ceiling</td>
<td>The Cisco logo should be pointing to the floor. Elevation: 0 degrees.</td>
</tr>
<tr>
<td>1240 mounted on the ceiling</td>
<td>The antenna should be perpendicular to the access point. Elevation: 0 degrees.</td>
</tr>
<tr>
<td>1240 mounted on the wall</td>
<td>The antenna should be parallel to the access point. Elevation: 0 degrees. If the antenna is perpendicular to the AP then the angle is 90 degrees (up or down does not matter as the dipole is omni).</td>
</tr>
</tbody>
</table>

Note

The access point must be mounted so that it is under 20 feet high. For best performance, a mounting at 10 feet would be ideal.

Following these guidelines makes it more likely that access points detect tracked devices. Rarely do two physical environments have the same RF characteristics. Users might need to adjust these parameters to their specific environment and requirements.

Note

Devices must be detected at signals greater than –75 dBm for the controllers to forward information to the location appliance. No fewer than three access points should be able to detect any device at signals below –75 dBm.

Note

If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in Prime Infrastructure. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees.

To use the Automatic Hierarchy Creation feature, you must have an established naming pattern for your wireless access points that provides the campus, building, floor, or outdoor area names for the maps. For example, San Jose-01-GroundFloor-AP3500i1.
Using the Automatic Hierarchy to Create Maps

**Step 1**
Choose **Maps > Automatic Hierarchy Creation** to display the Automatic Hierarchy Creation page.

**Step 2**
In the text box, enter the name of an access point on your system. Or, you can choose one from the list. This name is used to create a regular expression to create your maps.

Note
To update a previously created regular expression, click **Load and Continue** next to the expression and update the expression accordingly. To delete a regular expression, click **Delete** next to the expression.

**Step 3**
Click **Next**.

**Step 4**
If your access point’s name has a delimiter, enter it in the text box and click **Generate basic regex based on delimiter**. The system generates a regular expression that matches your access point’s name based on the delimiter.

For example, using the dash (-) delimiter in the access point name San Jose-01-GroundFloor-AP3500i1, produces the regular expression /(.*)-(.*)-(.*)-(.*)/.

If you have a more complicated access point name, you can manually enter the regular expression.

You are not required to enter the leading and trailing slashes.

As a convention, Prime Infrastructure displays regular expressions in slashes.

**Step 5**
Click **Test**. The system displays the maps that will be created for the access point name and the regular expression entered.

**Step 6**
Using the Group fields, assign matching groups to hierarchy types.

For example, if your access point is named: SJC14-4-AP-BREAK-ROOM

In this example, the campus name is SJC, the building name is 14, the floor name is 4, and the AP name is AP-BREAK-ROOM.

Use the regular expression: /([A-Z]+)(\d+)-(\d+)-(\d+)/

From the AP name, the following groups are extracted:

1. SJC
2. 14
3. 4
4. AP-BREAK-ROOM

The matching groups are assigned from left to right, starting at 1.

To make the matching groups match the hierarchy elements, use the drop-down list for each group number to select the appropriate hierarchy element.

This enables you to have almost any ordering of locations in your access point names.

For example, if your access point is named: EastLab-Atrium2-3-SanFrancisco

If you use the regular expression: /([^\d]+)(\d+)-(\d+)-(\d+)/

with the following group mapping:

1. Building
2. Device Name
3. Floor
4. Campus
Automatic Hierarchy Creation produces a campus named SanFrancisco, a building under that campus named EastLab, and a floor in EastLab named 3.

**Note**
The two hierarchy types, Not in device name and Device have no effect, but enable you to skip groups in case you need to use a matching group for some other purpose.

Automatic Hierarchy Creation requires the following groups to be mapped in order to compute a map on which to place the access point:

<table>
<thead>
<tr>
<th>Campus group present in match?</th>
<th>Building group present in match?</th>
<th>Floor group present in match?</th>
<th>Resulting location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Campus &gt; Building &gt; Floor</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Failed match</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Campus &gt; Floor (where Floor is an outdoor area)</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Failed match</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>System Campus &gt; Building &gt; Floor</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Failed match</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Failed match</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Failed match</td>
</tr>
</tbody>
</table>

Automatic Hierarchy Creation attempts to guess the floor index from the floor name. If the floor name is a number, AHC will assign the floor a positive floor index. If the floor name is a negative number or starts with the letter B (for example, b1, -4, or B2), AHC assigns the floor a negative floor index. This indicates that the floor is a basement.

When searching for an existing map on which to place the access point, AHC considers floors in the access point’s building with the same floor index as the access point’s name.

For example, if the map SF > MarketStreet > Sublevel1 exists and has a floor index of -1, then the access point SF-MarketStreet-b1-MON1 will be assigned to that floor.

**Step 7**
Click Next. You can test against more access points. You may test your regular expression and matching group mapping against more access points by entering the access point names in the Add more device names to test against field, and clicking Add.

You then click Test to test each of the access points names in the table. The result of each test is displayed in the table.

If required, return to the previous step to edit the regular expression or group mapping for the current regular expression.

**Step 8**
Click Next, then click Save and Apply. This applies the regular expression to the system. The system processes all the access points that are not assigned to a map.

**Note**
You can edit the maps to include floor images, correct dimensions, and so on. When Automatic Hierarchy Creation creates a map, it uses the default dimensions of 20 feet by 20 feet. You will need to edit the created maps to specify the correct dimensions and other attributes.
Maps created using Automatic Hierarchy Creation appear in the maps list with an *incomplete* icon. Once you have edited a map, the *incomplete* icon disappears. You may hide the column for incomplete maps by clicking the Edit View link.

---

**Using the Map Editor**

You use the Map Editor to define, draw, and enhance floor plan information. The map editor allows you to create obstacles so that they can be taken into consideration while computing RF prediction heatmaps for access points. You can also add coverage areas for location appliances that locate clients and tags in that particular area.

The planning mode opens the map editor in the browser window from which the planning tool is launched. If the original browser window has navigated away from the floor page, you need to navigate back to the floor page to launch the map editor.

- **Guidelines for Using the Map Editor**
- **Guidelines for Placing Access Points**
- **Guidelines for Inclusion and Exclusion Areas on a Floor**
- **Opening the Map Editor**
- **Map Editor Icons**
- **Using the Map Editor to Draw Coverage Areas**
- **Using the Map Editor to Draw Obstacles**
- **Defining an Inclusion Region on a Floor**
- **Defining an Exclusion Region on a Floor**
- **Defining a Rail Line on a Floor**

**Guidelines for Using the Map Editor**

Consider the following when modifying a building or floor map using the map editor:

- We recommend that you use the map editor to draw walls and other obstacles rather than importing an .FPE file from the legacy floor plan editor.
  - If necessary, you can still import .FPE files. To do so, navigate to the desired floor area, choose **Edit Floor Area** from the **Select a command** drop-down list, click **Go**, select the **FPE File** check box, and browse to choose the .FPE file.

- You can add any number of walls to a floor plan with the map editor; however, the processing power and memory of a client workstation might limit the refresh and rendering aspects of Prime Infrastructure.
  - We recommend a practical limit of 400 walls per floor for machines with 1 GB RAM or less.

- All walls are used by Prime Infrastructure when generating RF coverage heatmaps.
Guidelines for Placing Access Points

Place access points along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. Access points placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other access points.

*Figure 42-3  Access Points Clustered Together*

By increasing overall access point density and moving access points towards the perimeter of the coverage area, location accuracy is greatly improved.

*Figure 42-4  Improved Location Accuracy by Increasing Density*

In long and narrow coverage areas, avoid placing access points in a straight line. Stagger them so that each access point is more likely to provide a unique snapshot of a device location.

*Figure 42-5  Refrain From Straight Line Placement*
Although the design might provide enough access point density for high bandwidth applications, location suffers because each access point view of a single device is not varied enough; therefore, location is difficult to determine.

Move the access points to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.

*Figure 42-6 Improved Location Accuracy by Staggering Around Perimeter*

Most current wireless handsets support only 802.11b/n, which offers only three non-overlapping channels. Therefore, wireless LANs designed for telephony tend to be less dense than those planned to carry data. Also, when traffic is queued in the Platinum QoS bucket (typically reserved for voice and other latency-sensitive traffic), lightweight access points postpone their scanning functions that allow them to peak at other channels and collect, among other things, device location information. The user has the option to supplement the wireless LAN deployment with access points set to monitor-only mode. Access points that perform only monitoring functions do not provide service to clients and do not create any interference. They simply scan the airwaves for device information.

Less dense wireless LAN installations, such as voice networks, find their location accuracy greatly increased by the addition and proper placement of monitor access points.

*Figure 42-7 Less Dense Wireless LAN Installations*

Verify coverage using a wireless laptop, handheld, or phone to ensure that no fewer than three access points are detected by the device. To verify client and asset tag location, ensure that the Prime Infrastructure reports client devices and tags within the specified accuracy range (10 m, 90%).

**Note** If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in Prime Infrastructure. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees.

**Guidelines for Inclusion and Exclusion Areas on a Floor**

Inclusion and exclusion areas can be any polygon shape and must have at least three points.
You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to Prime Infrastructure. The inclusion region is indicated by a solid aqua line, and generally outlines the region.

You can define multiple exclusion regions on a floor.

Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

**Opening the Map Editor**

Follow these steps to use the map editor:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose <strong>Maps &gt; Site Map Design</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click the desired campus. The Site Maps &gt; Campus Name page appears.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click a campus and then click a building.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click the desired floor area. The Site Maps &gt; Campus Name &gt; Building Name &gt; Floor Area Name page appears.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>From the <strong>Select a command</strong> drop-down list, choose <strong>Map Editor</strong>, and click <strong>Go</strong>. The Map Editor page appears.</td>
</tr>
</tbody>
</table>

**Map Editor Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Scale Floor" /></td>
<td>Scale Floor—Click anywhere on the map to start drawing line. Double click to finish the line and enter the new line length in the popup shown. This will modify the floor dimensions to the new dimensions.</td>
</tr>
<tr>
<td><img src="image" alt="Measure Distance" /></td>
<td>Measure Distance—Click anywhere on the map to start drawing line. Double click to finish the line. Measured line length in ft/meters is shown on the top.</td>
</tr>
<tr>
<td><img src="image" alt="Copy/Move Obstacles" /></td>
<td>Copy/Move Obstacles—Select obstacles either by drawing a box on the map or by clicking the obstacles. To copy obstacles, click <strong>Copy</strong>. This will create new obstacles just above the selected obstacles. To move the obstacles, drag the selected obstacles to new position. Clicking anywhere on the map will unselect all the elements.</td>
</tr>
<tr>
<td><img src="image" alt="Delete Mode" /></td>
<td>Delete Mode—Select the elements to be deleted either by drawing a box on the map or clicking each element. Use Shift key to select multiple elements. Use the Ctrl key to toggle selection of elements, one at a time. Clicking anywhere on the map will unselect all the elements. Click <strong>Delete</strong> to delete the selected elements</td>
</tr>
<tr>
<td><img src="image" alt="Modify Mode" /></td>
<td>Modify Mode—Click an element and click the vertices to reshape or drag the element to move to a new position. Clicking anywhere on the map will unselect the selected element.</td>
</tr>
<tr>
<td><img src="image" alt="Draw Coverage Area" /></td>
<td>Draw Coverage Area</td>
</tr>
</tbody>
</table>
If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a coverage area.

**Step 1**
Add the floor plan if it is not already represented in Prime Infrastructure.

**Step 2**
Choose Maps > Site Maps.

**Step 3**
Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.

**Step 4**
From the Select a command drop-down list, choose Map Editor, and click Go.

**Step 5**
It the Map Editor page, click the Draw Coverage Area icon on the toolbar.

A pop-up appears.

**Step 6**
Enter the name of the area that you are defining. Click OK.

A drawing tool appears.

**Step 7**
Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.
- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

The outlined area must be a closed object to appear highlighted on the map.

**Step 8**
Click the disk icon on the toolbar to save the newly drawn area.

---

**Table 42-7** Next Generation Maps Icons (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌈</td>
<td>Draw Location Region</td>
</tr>
<tr>
<td>🌧️</td>
<td>Draw Rail</td>
</tr>
<tr>
<td>⚠️</td>
<td>Draw Obstacle—Click anywhere on the map to start drawing. Double click to finish drawing. Use Ctrl-z to undo, Ctrl-y to redo and ‘Esc’ key to cancel the current drawing.</td>
</tr>
<tr>
<td>✧</td>
<td>Place Marker</td>
</tr>
<tr>
<td>🚦</td>
<td>Navigation—Remove any selected modes such as drawing or editing and switches to navigation mode where you can view the map and perform zooming or panning.</td>
</tr>
</tbody>
</table>
Using the Map Editor to Draw Obstacles

Table 42-8 describes the obstacle color coding.

<table>
<thead>
<tr>
<th>Type of obstacle</th>
<th>Color coding</th>
<th>Loss (in dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thick wall</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>Light wall</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Heavy door</td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>Light door</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Cubicle</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Glass</td>
<td></td>
<td>1.5</td>
</tr>
</tbody>
</table>

Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

Step 1  Choose Maps > Site Maps.
Step 2  Click the name of the appropriate floor area.
Step 3  From the Select a command drop-down list, choose Map Editor.
Step 4  Click Go.
Step 5  At the map, click the aqua box on the toolbar.
A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.
Step 6  Click OK in the message box that appears. A drawing icon appears to outline the inclusion area.
Step 7  To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.
Step 8  Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.
Step 9  Repeat Step 8 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.
Step 10  Choose Save from the Command menu or click the disk icon on the toolbar to save the inclusion region.
Using the Map Editor

Note
If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 11
Select the Location Regions check box if it is not already selected. If you want it to apply to all floor maps, click Save settings. Close the Layers configuration page.

Step 12
To resynchronize Prime Infrastructure and MSE databases, choose Services > Synchronize Services.

Note
If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 13
In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Note
Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Step 1
Choose Maps > Site Maps.

Step 2
Click the name of the appropriate floor area.

Step 3
From the Select a command drop-down list, choose Map Editor.

Step 4
Click Go.

Step 5
At the map, click the purple box on the toolbar.

Step 6
Click OK in the message box that appears. A drawing icon appears to outline the exclusion area.

Step 7
To begin defining the exclusion area, move the drawing icon to the starting point on the map, and click once.

Step 8
Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.

Step 9
Repeat Step 8 until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.

Step 10
To define additional exclusion regions, repeat Step 5 to Step 9.
Step 11 When all exclusion areas are defined, choose Save from the Command menu or click the disk icon on the toolbar to save the exclusion region.

To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 12 Select the Location Regions check box if it is not already selected, click Save settings, and close the Layers configuration page when complete.

Step 13 To resynchronize Prime Infrastructure and location databases, choose Services > Synchronize Services.

Step 14 In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

---

**Defining a Rail Line on a Floor**

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

*Note* Rail line configurations do not apply to tags.

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

To define a rail with a floor, follow these steps:

- **Step 1** Choose Maps > Site Maps.
- **Step 2** Click the name of the appropriate floor area.
- **Step 3** Choose Map Editor from the Select a command drop-down list.
- **Step 4** Click Go.
- **Step 5** In the map, click the rail icon (to the right of the purple exclusion icon) on the toolbar.
- **Step 6** In the message dialog box that appears, enter a snap-width (feet or meters) for the rail and then click OK. A drawing icon appears.
- **Step 7** Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.
- **Step 8** Click the drawing icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

- **Step 9** At the floor map, choose the Layers drop-down list.
- **Step 10** Select the Rails check box if it is not already selected, click Save settings, and close the Layers configuration pane when complete.
Adding an Outdoor Area

You can add an outdoor area to a campus map in the Prime Infrastructure database regardless of whether you have added outdoor area maps to the database.

To add an outdoor area to a campus map, follow these steps:

Step 1 If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.

Note You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because Prime Infrastructure automatically resizes the map to fit the workspace.

Step 2 Choose Maps > Site Maps.

Step 3 Click the desired campus to display the Monitor > Site Maps > Campus View page.

Step 4 From the Select a command drop-down list, choose New Outdoor Area.

Step 5 Click Go. The Create New Area page appears.

Step 6 In the New Outdoor Area page, enter the following information:

- Name—The user-defined name of the new outdoor area.
- Contact—The user-defined contact name.
- Area Type (RF Model)—Cubes And Walled Offices, Drywall Office Only, Outdoor Open Space (default).
- AP Height (feet)—Enter the height of the access point.
- Image File—Name of the file containing the outdoor area map. Click Browse to find the file.

Step 7 Click Next.

Step 8 Click Place to put the outdoor area on the campus map. Prime Infrastructure creates an outdoor area rectangle scaled to the size of the campus map.

Step 9 Click and drag the outdoor area rectangle to the desired position on the campus map.

Step 10 Click Save to save this outdoor area and its campus location to the database.

A hyperlink associated with the outdoor area takes you to the corresponding Maps page.

Step 11 (Optional) To assign location presence information for the new outdoor area, choose Edit Location Presence Info, and click Go.
By default, the Override Child Element Presence Info check box is selected. There is no need to alter this setting for outdoor areas.

Using Chokepoints to Enhance Tag Location Reporting

Installation of chokepoints provides enhanced location information for RFID tags. When an active Cisco-compatible Extensions Version 1-compliant RFID tag enters the range of a chokepoint, it is stimulated by the chokepoint. The MAC address of this chokepoint is then included in the next beacon sent by the stimulated tag. All access points that detect this tag beacon then forward the information to the controller and location appliance.

Using chokepoints in conjunction with active compatible extensions compliant tags provides immediate location information on a tag and its asset. When a Cisco-compatible Extension tag moves out of the range of a chokepoint, its subsequent beacon frames do not contain any identifying chokepoint information. Location determination of the tag defaults to the standard calculation methods based on RSSIs reported by the access point associated with the tag.

- Adding a Chokepoint to a Prime Infrastructure Map
- Positioning Chokepoints
- Adding Wi-Fi TDOA Receivers to Prime Infrastructure
- Adding Wi-Fi TDOA Receivers to a Map
- Positioning Wi-Fi TDOA Receivers
- Managing RF Calibration Models

Adding Chokepoints to Prime Infrastructure

Chokepoints are installed and configured as recommended by the Chokepoint vendor. After the chokepoint installation is complete and operational, the chokepoint can be entered into the location database and plotted on an Prime Infrastructure map.

To add a chokepoint to the Prime Infrastructure database, follow these steps:

Step 1 Choose Configure > Chokepoints.
Step 2 From the Select a command drop-down list, choose Add Chokepoints.
Step 3 Click Go.
Step 4 Enter the MAC address and name for the chokepoint.
Step 5 Select the Entry/Exit Chokepoint check box.
Step 6 Enter the coverage range for the chokepoint.

The Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7 Click OK.
After the chokepoint is added to the database, it can be placed on the appropriate Prime Infrastructure floor map.

## Adding a Chokepoint to a Prime Infrastructure Map

To add the chokepoint to a map, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** In the Maps page, choose the link that corresponds to the floor location of the chokepoint.

**Step 3** From the Select a command drop-down list, choose Add Chokepoints.

**Step 4** Click Go.

The Add Chokepoints summary page lists all recently added chokepoints that are in the database but are not yet mapped.

**Step 5** Select the check box next to the chokepoint that you want to place on the map.

**Step 6** Click OK.

A map appears with a chokepoint icon located in the top left-hand corner. You are now ready to place the chokepoint on the map.

**Step 7** Left-click the chokepoint icon and drag it to the proper location.

The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

**Step 8** Click Save.

You are returned to the floor map and the added chokepoint appears on the map.

---

**Note** The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

**Note** The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

**Note** The MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint appear when you hover your mouse cursor over its map icon.

**Step 9** If the chokepoint does not appear on the map, select the Chokepoints check box located in the Floor Settings menu.

---

**Note** Do not click Save Settings unless you want to save this display criteria for all maps.
You must synchronize the network design to the mobility services engine or location server to push chokepoint information.

**Positioning Chokepoints**

To position chokepoints on the map, follow these steps:

**Step 1**
Left-click the Chokepoint icon and drag it to the proper location.

The MAC address, name, and coverage range of the chokepoint appear in the dialog box in the left when you click the chokepoint icon for placement.

**Step 2**
Click Save when the icon is correctly placed on the map.

**Step 3**
The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor.

**Note**
The rings around the chokepoint icon indicate the coverage area. When a Cisco-compatible Extensions tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. The chokepoint range is provided as a visual only, but chokepoint vendor software is required to actually configure the range. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

**Note**
The MAC address, name, and range of a chokepoint are displayed when you hover your mouse cursor over its map icon.

**Step 4**
If the chokepoint does not appear on the map, choose Layers to view a drop-down list of possible elements to display on the map. Select the Chokepoints check box.

**Note**
Do not click Save Settings unless you want to save this display criteria for all maps.

**Note**
You can change the position of chokepoints by importing or exporting a file.

**Configuring Wi-Fi TDOA Receivers**

- Adding Wi-Fi TDOA Receivers to Prime Infrastructure
- Adding Wi-Fi TDOA Receivers to a Map
- Positioning Wi-Fi TDOA Receivers
- Managing RF Calibration Models
### Adding Wi-Fi TDOA Receivers to Prime Infrastructure

To add Wi-Fi TDOA receivers to the Prime Infrastructure database, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Configure &gt; WiFi TDOA Receivers.</td>
</tr>
<tr>
<td>2</td>
<td>From the Select a command drop-down list, choose Add WiFi TDOA Receivers.</td>
</tr>
<tr>
<td>3</td>
<td>Click Go.</td>
</tr>
<tr>
<td>4</td>
<td>Enter the MAC address, name, and static IP address for the Wi-Fi TDOA receiver.</td>
</tr>
<tr>
<td>5</td>
<td>Click OK to save the Wi-Fi TDOA receiver entry to the database.</td>
</tr>
</tbody>
</table>

**Note**: Wi-Fi TDOA receivers are configured separately using the Wi-Fi TDOA receiver vendor software.

After the Wi-Fi TDOA receiver is added to the database, place it on the appropriate Prime Infrastructure floor map. See the “Adding Wi-Fi TDOA Receivers to Prime Infrastructure” section on page 42-xlvi for more information.

### Adding Wi-Fi TDOA Receivers to a Map

To add a WiFi TDOA receiver to a map, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Maps &gt; Site Maps.</td>
</tr>
<tr>
<td>2</td>
<td>Choose the link that corresponds to the floor location of the Wi-Fi TDOA receiver.</td>
</tr>
<tr>
<td>3</td>
<td>From the Select a command drop-down list, choose Add WiFi TDOA Receivers.</td>
</tr>
<tr>
<td>4</td>
<td>Click Go.</td>
</tr>
</tbody>
</table>

The Add WiFi TDOA Receivers summary page lists all recently added Wi-Fi TDOA receivers that are in the database but are not yet mapped.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Select the check box next to the Wi-Fi TDOA receiver to be added to the map.</td>
</tr>
<tr>
<td>6</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>

A map appears with a green WiFi TDOA receiver icon located in the top left-hand corner. You are now ready to position the Wi-Fi TDOA receiver on the map.

### Positioning Wi-Fi TDOA Receivers

To position Wi-Fi TDOA receivers on the map, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Left-click the WiFi TDOA receiver icon and drag it to the proper location.</td>
</tr>
</tbody>
</table>
The MAC address and name of the Wi-Fi TDOA receiver appear in the left pane when you click the Wi-Fi TDOA receiver icon for placement.

**Step 2**
Click **Save** when the icon is correctly placed on the map.
The MAC address of the Wi-Fi TDOA receiver appears when you hover your mouse cursor over its map icon.

**Step 3**
If the chokepoint does not appear on the map, click **Layers** to view a drop-down list of possible elements to display on the map. Select the **WiFi TDOA Receivers** check box.

---

**Note**
Do not select **Save Settings** unless you want to save this display criteria for all maps.

---

**Note**
You can change the position of Wi-Fi TDOA Receivers by importing or exporting a file.

---

**Related Topics**
- Adding Wi-Fi TDOA Receivers to Prime Infrastructure
- Adding Wi-Fi TDOA Receivers to a Map
- Positioning Wi-Fi TDOA Receivers

### Managing RF Calibration Models

If the provided RF models do not sufficiently characterize the floor layout, you can create a calibration model that is applied to the floor and better represents the attenuation characteristics of that floor. The calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. This enables the Cisco WLAN solution installation team to lay out one floor in a multi-floor area, use the RF calibration tool to measure, save the RF characteristics of that floor as a new calibration model, and apply that calibration model to all the other floors with the same physical layout.

You can collect data for a calibration using one of two methods:

- **Point mode data collection**—Calibration points are selected and their coverage area is calculated one location at a time.
- **Linear mode data collection**—A series of linear paths are selected and then calculated as you traverse the path. This approach is generally faster than the point mode data collection. You can also employ point mode data collection to augment data collection for locations missed by the linear paths.

---

**Note**
Calibration models can only be applied to clients, rogue clients, and rogue access points. Calibration for tags is done using the Aeroscout System Manager. See the following URL for details on tag calibration at: [http://support.aeroscout.com](http://support.aeroscout.com).

---

**Note**
We recommend client device that supports both 802.11a/n and 802.11b/g/n radios to expedite the calibration process for both spectrums.
Use a laptop or other wireless device to open a browser to Prime Infrastructure server and perform the calibration process.

- Accessing Current Calibration Models
- Applying Calibration Models to Maps
- Viewing Calibration Model Properties
- Viewing Calibration Model Details
- Creating New Calibration Models
- Starting Calibration Process
- Calibrating
- Apply the Model to the Floor
- Deleting Calibration Models

**Accessing Current Calibration Models**

To access current calibration models, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** From the Select a command drop-down list, choose RF Calibration Models. The Model Name and Status for each calibration model are listed.

**Step 3** Click the model name to access a specific calibration model.

**Related Topics**

- Accessing Current Calibration Models
- Applying Calibration Models to Maps
- Viewing Calibration Model Properties
- Viewing Calibration Model Details
- Creating New Calibration Models
- Starting Calibration Process
- Calibrating
- Apply the Model to the Floor
- Deleting Calibration Models

**Applying Calibration Models to Maps**

To apply a current calibration model to a map, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** From the Select a command drop-down list, choose RF Calibration Models.

**Step 3** Click the model name to access the applicable calibration model.

**Step 4** From the Select a command drop-down list, choose Apply to Maps.
Step 5  Click Go.

Related Topics
- Accessing Current Calibration Models
- Viewing Calibration Model Properties
- Viewing Calibration Model Details
- Creating New Calibration Models
- Starting Calibration Process
- Apply the Model to the Floor
- Deleting Calibration Models

Viewing Calibration Model Properties

To view or edit current calibration models, follow these steps:

Step 1  Choose Maps > Site Maps.
Step 2  From the Select a command drop-down list, choose RF Calibration Models.
Step 3  Click the model name to access the applicable calibration model.
Step 4  From the Select a command drop-down list, choose Properties.
Step 5  Click Go to view or edit calibration model details. See the Viewing Calibration Model Properties for more information.

Related Topics
- Accessing Current Calibration Models
- Applying Calibration Models to Maps
- Viewing Calibration Model Details
- Creating New Calibration Models
- Starting Calibration Process
- Apply the Model to the Floor
- Deleting Calibration Models

Viewing Calibration Model Details

To edit calibration model details, follow these steps:

Step 1  Choose Maps > Site Maps.
Step 2  From the Select a command drop-down list, choose RF Calibration Models.
Step 3  Click the model name to access the applicable calibration model.
Step 4  From the Select a command drop-down list, choose Properties.
Step 5  Click Go.

Step 6  The following parameters might be edited:
   - Sweep Client Power for Location—Click to enable. You might want to enable this if a high density of access points exists and transmit power is reduced or unknown. The sweeping range of client transmit power might improve accuracy but scalability is negatively affected.
   - HeatMap Binsize—Choose 4, 8, 16, or 32 from the drop-down list.
   - HeatMap Cutoff—Determine the heatmap cutoff. We recommend a low heatmap cutoff especially if the access point density is high and RF propagation conditions are favorable. A higher cutoff value increases scalability but might cause difficulty when locating clients.

Step 7  When any necessary changes have been made or to exit the page, click OK.

Related Topics
- Accessing Current Calibration Models
- Applying Calibration Models to Maps
- Viewing Calibration Model Properties
- Creating New Calibration Models
- Starting Calibration Process
- Apply the Model to the Floor
- Deleting Calibration Models

Creating New Calibration Models

To create a new calibration model, follow these steps:

Step 1  Choose Maps > Site Maps.
Step 2  From the Select a command drop-down list, choose RF Calibration Models.
Step 3  Click Go.
Step 4  From the Select a command drop-down list, choose Create New Model.
Step 5  Click Go.
Step 6  Enter a model name, and click OK.

The new model appears along with the other RF calibration models with a status of Not Yet Calibrated.

Related Topics
- Accessing Current Calibration Models
- Applying Calibration Models to Maps
- Viewing Calibration Model Properties
- Viewing Calibration Model Details
- Starting Calibration Process
- Apply the Model to the Floor
Starting Calibration Process

To start the calibration process, follow these steps:

Step 1  Click the model name to open the Calibration Model > Model Name page.
Step 2  From the Select a command drop-down list, choose Add Data Points.
Step 3  Click Go.
Step 4  Enter the MAC address of the device being used to perform the calibration. Manually-entered MAC addresses must be delimitied with colons (such as FF:FF:FF:FF:FF:FF).

Note If this process is being performed from a mobile device connected to Prime Infrastructure through the Cisco Centralized architecture, the MAC address text box is automatically populated with the device address.

Step 5  Choose the appropriate campus, building, floor, or outdoor area where the calibration is performed.

Note The calibration in the outdoor area is supported in Release 1.0.x and later. You can use this option to add the calibration data points to the outdoor area. The data points can be added to the outdoor area using the same procedure for calibration.

Step 6  Click Next.
Step 7  When the chosen floor map and access point locations appear, a grid of plus marks (+) indicates the locations where data collection for calibration is performed.

Using these locations as guidelines, you can perform either a point or linear collection of data by appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that appear on the map when the respective options are displayed.

If you want to perform a point collection of data for the calibration, do the following:

a. Choose Point from the Collection Method drop-down list and select the Show Data points check box if not already selected. A calibration point pop-up appears on the map.

b. Position the tip of the calibration point pop-up at a data point (+), and click Go. A dialog box appears showing the progress of the data collection.

Note Rotate the calibrating client laptop during data collection so that the client is heard evenly by all access points in the vicinity.

c. When the data collection is complete for a selected data point and the coverage area is plotted on the map, move the calibration point pop-up to another data point, and click Go.

Note The coverage area plotted on the map is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in legend on the left side of the page. Additionally, the progress of the calibration process is indicated by two status bars above the legend, one for 802.11a/n and one for 802.11b/g/n.
d. Repeat point collection Steps a. to c. until the calibration status bar of the relevant spectrums (802.11a/n, 802.11b/g/n) display as ‘done.’

Note The calibration status bar indicates data collection for the calibration as done after roughly 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802.11a/n.

If you want to perform a linear collection of data for the calibration, do the following:

a. Choose Linear from the Collection Method drop-down list, and select the Show Data points check box if not already selected. A line appears on the map with both Start and Finish pop-ups.

b. Position the tip of the Start pop-up at the starting data point.

c. Position the Finish pop-up at the ending data point.

d. Position yourself with your laptop at the starting data point, and click Go. Walk steadily towards the end point along the defined path. A dialog box appears to show that data collection is in process.

Note Do not stop data collection until you reach the end point even if the data collection bar indicates completion.

Note Only Intel and Cisco adapters have been tested. Make sure Enable Cisco-compatible Extensions and Enable Radio Management Support are enabled in the Cisco-compatible Extension Options.

e. Press the space bar (or Done on the data collection panel) when you reach the end point. The collection pane displays the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected.

f. Repeat linear collection Steps b to e until the status bar for the respective spectrum is filled in (done).
### Step 8
Click the name of the calibration model at the top of the page to return to the main page for that model to calibrate the data points.

### Step 9
Choose **Calibrate** from the Select a command drop-down list, and click **Go**.

### Step 10
Click the **Inspect Location Quality** link when calibration completes. A map displays showing RSSI readings displays.

### Step 11
To use the newly created calibration model, you must apply the model to the floor on which it was created (and on any other floors with similar attenuation characteristics as well). Choose **Monitor > Site Maps** and find the specific floor to which the model is applied. At the floor map interface, choose **Edit Floor Area** from the drop-down list, and click **Go**.

### Step 12
From the Floor Type (RF Model) drop-down list, choose the newly created calibration model. Click **OK** to apply the model to the floor.

This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all location determination performed on that floor is done using the specific collected attenuation data from the calibration model.

---

### Related Topics
- Accessing Current Calibration Models
- Applying Calibration Models to Maps
- Viewing Calibration Model Properties
- Viewing Calibration Model Details
- Creating New Calibration Models
- Apply the Model to the Floor
- Deleting Calibration Models

---

### Calibrating
To compute the collected data points, follow these steps:

### Step 1
Click the model name to open the Calibration Model > Model Name page.

### Step 2
In the Calibration Model > Model Name page, choose **Calibrate** from the Select a command drop-down list.

### Step 3
Click **Go**.

---

### Apply the Model to the Floor
To use the newly created calibration model, you must apply the model to the floor on which it was created (along with other floors with similar attenuation characteristics).
To apply the model to the floor, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Maps &gt; Site Maps</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Locate the specific floor to which the model is applied.</td>
</tr>
<tr>
<td>3</td>
<td>From the Select a command drop-down list, choose <strong>Edit Floor Area</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Go</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>From the Floor Type (RF Model) drop-down list, choose the newly-created calibration model.</td>
</tr>
<tr>
<td>6</td>
<td>Click <strong>OK</strong> to apply the model to the floor.</td>
</tr>
</tbody>
</table>

This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all location determination performed on that floor is done using the specific collected attenuation data from the calibration model.

**Related Topics**

- Accessing Current Calibration Models
- Applying Calibration Models to Maps
- Viewing Calibration Model Properties
- Viewing Calibration Model Details
- Creating New Calibration Models
- Starting Calibration Process
- Deleting Calibration Models

### Deleting Calibration Models

To delete a calibration model, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click the model name to open the Calibration Model &gt; Model Name page.</td>
</tr>
<tr>
<td>2</td>
<td>From the Select a command drop-down list, choose <strong>Delete Model</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Go</strong>.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Accessing Current Calibration Models
- Applying Calibration Models to Maps
- Viewing Calibration Model Properties
- Viewing Calibration Model Details
- Creating New Calibration Models
- Starting Calibration Process
- Apply the Model to the Floor
Managing Location Presence Information

You can enable location presence through mobility services engine to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by clients on a demand basis for use by location-based services and applications.

To view or edit current location presence information for a current map, follow these steps:

1. Choose Maps > Site Maps.
2. Select the check box of the map.
3. From the Select a command drop-down list, choose Location Presence.
4. Click Go.

The Location Presence page appears.

To view the current map location information (Area Type, Campus, Building, and Floor) see the map you selected in the Maps > Site Maps page. To select a different map, use the Select a Map to Update Presence Information drop-down lists to choose the new map location.

5. Click the Civic Address, GPS Markers, or Advanced tab.
   - Civic Address—Identifies the campus, building, or floor by name, street, house number, house number suffix, city (address line2), state, postal code, and country.
   - GPS Markers—Identify the campus, building, or floor by longitude and latitude.
   - Advanced—Identifies the campus, building, or floor with expanded civic information such as neighborhood, city division, county, and postal community name.

Each selected field is inclusive of all of those above it. For example, if you select Advanced, it can also provide GPS and Civic location information upon client demand. The selected setting must match what is set on the mobility services engine level.

If a client requests location information such as GPS Markers for a campus, building, floor, or outdoor area that is not configured for that field, an error message appears.

By default, the Override Child Element Presence Info check box is selected.

Searching Maps

You can use the following parameters in the Search Maps page:

- Search for
- Map Name
- Search in
- Save Search
- Items per page

After you click Go, the map search results page appears (see Table 42-9).
Using Wireless Maps

Chapter 42

Using the Map Editor

You can use the Prime Infrastructure map editor to define, draw, and enhance floor plan information.

- Opening the Map Editor
- Defining a Rail Line on a Floor
- Defining an Inclusion Region on a Floor
- Defining an Exclusion Region on a Floor
- Defining a Rail Line on a Floor

Opening the Map Editor

Follow these steps to use the map editor:

**Step 1** Choose Maps > Site Maps to display the Maps page.
**Step 2** Click the desired campus. The Site Maps > Campus Name page appears.
**Step 3** Click a campus and then click a building.
**Step 4** Click the desired floor area. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.
**Step 5** From the Select a command drop-down list, choose Map Editor, and click Go. The Map Editor page appears.

**Note** Make sure that the floor plan images are properly scaled so that all white space outside of the external walls is removed. To make sure that floor dimensions are accurate, click the compass tool on the toolbar.
Using the Map Editor

Step 6  Position the reference length. When you do, the Scale menu appears with the line length supplied. Enter the dimensions (width and height) of the reference length, and click **OK**.

Step 7  Determine the propagation pattern from the Antenna Mode drop-down list.

Step 8  Make antenna adjustments by sliding the antenna orientation bar to the desired degree of direction.

Step 9  Choose the desired access point.

Step 10  Click **Save**.

**Related Topics**

- Defining a Rail Line on a Floor
- Defining an Inclusion Region on a Floor
- Defining an Exclusion Region on a Floor
- Defining a Rail Line on a Floor

**Using the Map Editor to Draw Polygon Areas**

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a polygon-shaped area.

Step 1  Add the floor plan if it is not already represented in Prime Infrastructure (see the [Adding Floor Areas to Buildings](#)).

Step 2  Choose **Maps > Site Maps**.

Step 3  Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.

Step 4  From the **Select a command** drop-down list, choose **Map Editor**, and click **Go**.

Step 5  In the Map Editor page, click the **Add Perimeter** icon on the toolbar.

- A pop-up appears.

Step 6  Enter the name of the area that you are defining. Click **OK**.

- A drawing tool appears.

Step 7  Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.
- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

The outlined area must be a closed object to appear highlighted on the map.

Step 8  Click the disk icon on the toolbar to save the newly drawn area.

Step 9  Choose **Command > Exit** to close the window. You are returned to the original floor plan.

**Note**  When you return to the original floor plan view after exiting the map editor, the newly drawn area is not visible; however, it appears in the Planning Model page when you add elements.

Step 10  Choose **Planning Mode** from the Select a command drop-down list to begin adding elements to the newly defined polygon-shaped area. See Table 42-8 for the obstacle color coding.
The RF prediction heatmaps for access points approximate the actual RF signal intensity. It takes into account the attenuation of obstacles drawn using the Map Editor but it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions. The thick wall (color-coded orange) with a loss of 13 dB might not be enough to contain the RF signal beyond the walls of the heatmap.

### Related Topics
- Opening the Map Editor
- Defining an Inclusion Region on a Floor
- Defining an Exclusion Region on a Floor
- Defining a Rail Line on a Floor

### Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

**Step 1** Choose **Maps > Site Maps**.

**Step 2** Click the name of the appropriate floor area.

**Step 3** From the Select a command drop-down list, choose **Map Editor**.

**Step 4** Click **Go**.

**Step 5** At the map, click the aqua box on the toolbar. A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.

**Step 6** Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

**Step 7** To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

**Step 8** Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

**Step 9** Repeat **Step 8** until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.

**Step 10** Choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the inclusion region.

**Note** If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

**Step 11** To return to the floor map to enable inclusion regions on heatmaps, choose **Exit** from the Command menu.

**Step 12** Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page.
Step 13 To resynchronize Prime Infrastructure and MSE databases, choose Services > Synchronize Services.

Note If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 14 In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Related Topics
- Opening the Map Editor
- Defining a Rail Line on a Floor
- Defining an Exclusion Region on a Floor
- Defining a Rail Line on a Floor

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Step 1 Choose Maps > Site Maps.
Step 2 Click the name of the appropriate floor area.
Step 3 From the Select a command drop-down list, choose Map Editor.
Step 4 Click Go.
Step 5 At the map, click the purple box on the toolbar.
Step 6 Click OK in the message box that appears. A drawing icon appears to outline the exclusion area.
Step 7 To begin defining the exclusion area, move the drawing icon to the starting point on the map, and click once.
Step 8 Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.
Step 9 Repeat Step 8 until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.
Step 10 To define additional exclusion regions, repeat Step 5 to Step 9.
Step 11 When all exclusion areas are defined, choose Save from the Command menu or click the disk icon on the toolbar to save the exclusion region.
Note
To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 12 To return to the floor map to enable exclusion regions on heatmaps, choose Exit from the Command menu.

Step 13 Select the Location Regions check box if it is not already selected, click Save settings, and close the Layers configuration page when complete.

Step 14 To resynchronize Prime Infrastructure and location databases, choose Services > Synchronize Services.

Step 15 In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Related Topics
- Opening the Map Editor
- Defining a Rail Line on a Floor
- Defining an Inclusion Region on a Floor
- Defining a Rail Line on a Floor

Defining a Rail Line on a Floor

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

Note
Rail line configurations do not apply to tags.

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

To define a rail with a floor, follow these steps:

Step 1 Choose Maps > Site Maps.
Step 2 Click the name of the appropriate floor area.
Step 3 Choose Map Editor from the Select a command drop-down list.
Step 4 Click Go.
Step 5 In the map, click the rail icon (to the right of the purple exclusion icon) on the toolbar.
Step 6 In the message dialog box that appears, enter a snap-width (feet or meters) for the rail and then click OK. A drawing icon appears.
Step 7 Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.
Step 8  Click the **drawing** icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

**Note**  To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 9  To return to the floor map to enable rails on heatmaps, choose **Exit** from the Command menu.

Step 10  At the floor map, choose the **Layers** drop-down list.

Step 11  Select the **Rails** check box for if it is not already selected, click **Save settings**, and close the Layers configuration panel when complete.

Step 12  To resynchronize Prime Infrastructure and mobility services engine, choose **Services > Synchronize Services**.

Step 13  In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

**Related Topics**
- Opening the Map Editor
- Defining a Rail Line on a Floor
- Defining an Inclusion Region on a Floor
- Defining an Exclusion Region on a Floor

**Inspecting Location Readiness and Quality**

You can configure Prime Infrastructure to verify the ability of the existing access point deployment to estimate the true location of a client, rogue client, rogue access point, or tag within 10 meters at least 90% of the time. The location readiness calculation is based on the number and placement of access points.

You can also check the location quality and the ability of a given location to meet the location specification (10 m, 90%) based on data points gathered during a physical inspection and calibration.

**Inspecting Location Readiness**

The Inspect Location Readiness feature is a distance-based predictive tool that can point out problem areas with access point placement.

To access the Inspect Location Readiness tool, follow these steps:

**Step 1**  Choose **Maps > Site Maps**.

**Step 2**  Click the applicable floor area name to view the map.
Inspecting Location Readiness and Quality

Note
If RSSI is not displayed, you can enable AP Heatmaps by selecting the AP Heatmaps check box on the left sidebar menu.

Note
If clients, tags, and access points are not displayed, verify that their respective check boxes are selected on the left sidebar menu. Licenses for both clients and tags must also be purchased for each to be tracked.

Step 3
From the Select a command drop-down list, choose **Inspect Location Readiness**.

Step 4
Click **Go**.

A color-coded map appears showing those areas that meet (indicated by Yes) and do not meet (indicated by No) the ten meter, 90% location specification.

Inspecting Location Quality Using Calibration Data

After completing a calibration model based on data points generated during a physical tour of the area, you can inspect the location quality of the access points.

To inspect location quality based on calibration, follow these steps:

Step 1
Choose **Maps > Site Maps**.

Step 2
Choose **RF Calibration Model** from the Select a command list. Click **Go**.

A list of calibration models appears.

Step 3
Click the appropriate calibration model.

Details on the calibration including date of last calibration, number of data points by signal type (802.11a, 802.11 b/g) used in the calibration, location, and coverage are displayed.

Step 4
In the same page, click the **Inspect Location Quality** link found under the Calibration Floors heading.

A color-coded map noting percentage of location errors appears.

Note
You can modify the distance selected to see the effect on the location errors.

Related Topics

- Using Planning Mode
- Accessing Planning Mode
- Using Planning Mode to Calculate Access Point Requirements
Inspecting VoWLAN Readiness

The VoWLAN Readiness (voice readiness) tool allows you to check the RF coverage to determine if it is sufficient for your voice needs. This tool verifies RSSI levels after access points have been installed.

To access the VoWLAN Readiness Tool (VRT), follow these steps:

**Step 1**  Choose Maps > Site Maps.  
**Step 2**  Click the applicable floor area name.  
**Step 3**  From the Select a command drop-down list, choose Inspect VoWLAN Readiness.  
**Step 4**  Choose the applicable Band, AP Transmit Power, and Client parameters from the drop-down lists.  

![Note](By default, the region map displays the b/g/n band for Cisco Phone-based RSSI threshold. The new settings cannot be saved.)

**Step 5**  Depending on the selected client, the following RSSI values might not be editable:

- Cisco Phone—RSSI values are not editable.
- Custom—RSSI values are editable with the following ranges:
  - Low threshold between -95dBm to -45dBm
  - High threshold between -90dBm to -40dBm

**Step 6**  The following color schemes indicate whether or not the area is voice ready:

- Green—Yes
- Yellow—Marginal
- Red—No

![Note](The accuracy of the Green/Yellow/Red regions depends on the RF environment and whether or not the floor is calibrated. If the floor is calibrated, the accuracy of the regions is enhanced.)

Troubleshooting Voice RF Coverage Issues

- Floors with either calibration or no calibration data are treated as follows:
  - Set the AP Transmit field to Max (the maximum downlink power settings). If the map still shows some yellow or red regions, more access points are required to cover the floor.
  - If the calibrated model shows red or yellow regions (where voice is expected to be deployed) with the AP Transmit field set to Current, increasing the power level of the access points might help.
Monitoring Mesh Networks Using Maps

You can access and view details for the following elements from a mesh network map in Prime Infrastructure:

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

Details on how this information is accessed and displayed for each of these items is detailed in this section.

- Monitoring Mesh Link Statistics Using Maps
- Monitoring Mesh Access Points Using Maps
- Monitoring Mesh Access Point Neighbors Using Maps
- Viewing the Mesh Network Hierarchy Using Maps
- Using Mesh Filters to Modify Map Display of Maps and Mesh Links

Monitoring Mesh Link Statistics Using Maps

You can view the SNR for a specific mesh network link, view the number of packets transmitted and received on that link, and initiate a link test in the Maps > Site Maps page.

To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the map name that corresponds to the outdoor area, campus, building, or floor you want to monitor.

**Step 3** From the left sidebar menu, click the arrow to the right of AP Mesh Info. The Mesh Filter dialog box appears.

**Step 4** Move the cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 42-10 summarizes the parameters that appear.

The color of the dot also provides a quick reference point of the SNR strength as follows:

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

The Bridging Link information appears.

**Table 42-10 Bridging Link Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information fetched on</td>
<td>Date and time that information was compiled.</td>
</tr>
<tr>
<td>Link SNR</td>
<td>Link signal-to-noise ratio (SNR).</td>
</tr>
<tr>
<td>Link Type</td>
<td>Hierarchical link relationship.</td>
</tr>
</tbody>
</table>
Monitoring Mesh Networks Using Maps

Table 42-10  Bridging Link Information  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNR Up</td>
<td>Signal-to-noise radio for the uplink (dB).</td>
</tr>
<tr>
<td>SNR Down</td>
<td>Signal-to-noise radio for the downlink (dB).</td>
</tr>
<tr>
<td>PER</td>
<td>The packet error rate for the link.</td>
</tr>
<tr>
<td>Tx Parent Packets</td>
<td>The TX packets to a node while acting as a parent.</td>
</tr>
<tr>
<td>Rx Parent Packets</td>
<td>The RX packets to a node while acting as a parent.</td>
</tr>
<tr>
<td>Time of Last Hello</td>
<td>Date and time of last hello.</td>
</tr>
</tbody>
</table>

**Step 5**  
Click either Link Test, Child to Parent or Link Test, Parent to Child. After the link test is complete, a results page appears.

**Note**  
A link test runs for 30 seconds.

**Note**  
You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.

**Step 6**  
To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. A page with multiple SNR graphs appears.

The following graphs are displayed for the link:
- SNR Up—Plots the RSSI values of the neighbor from the perspective of the access point.
- SNR Down—Plots the RSSI values that the neighbor reports to the access point.
- Link SNR—Plots a weighed and filtered measurement based on the SNR Up value.
- The Adjusted Link Metric—Plots the value used to determine the least cost path to the root access point. This value represents the ease of getting the rooftop access point and accounts for the number of hops. The lower the ease value, the less likely the path is used.
- The Unadjusted Link Metric—Plots the least cost path to get to the root access point unadjusted by the number of hops. The higher the value for the unadjusted link, the better the path.

**Monitoring Mesh Access Points Using Maps**

You can view the following summary information for a mesh access point from a mesh network map:
- Parent
- Number of children
- Hop count
- Role
- Group name
- Backhaul interface
- Data Rate
Monitoring Mesh Networks Using Maps

To view summary and detailed configuration information for a mesh access point from a mesh network map, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the map name that corresponds to the outdoor area, campus, building, or floor location of the access point you want to monitor.

**Step 3** To view summary configuration information for an access point, hover your mouse cursor over the access point that you want to monitor. A dialog box with configuration information for the selected access point appears.

**Step 4** To view detailed configuration information for an access point, double-click the access point appearing on the map. The configuration details for the access point appear.

**Note** For more details on the View Mesh Neighbors link in the access point dialog box, see the Monitoring Mesh Access Point Neighbors Using Maps. If the access point has an IP address, a Run Ping Test link is also visible at the bottom of the mesh access point dialog box.

**Step 5** In the Access Point Details configuration page, follow these steps to view configuration details for the mesh access point:

a. Click the **General** tab to view the overall configuration of the mesh access point such as the AP name, MAC address, AP Up time, associated controllers (registered and primary) operational status, and software version.

**Note** The software version for mesh access points is appended with the letter m and the word mesh appears in parentheses.

b. Click the **Interface** tab to view configuration details for the interfaces supported on the mesh access point. Interface options are radio and Ethernet.

c. Click the **Mesh Links** tab to view parent and neighbor details (name, MAC address, packet error rate, and link details) for the mesh access point. You can also initiate link tests from this page.

d. Click the **Mesh Statistics** tab to view details on the bridging, queue, and security statistics for the mesh access point.

**Monitoring Mesh Access Point Neighbors Using Maps**

To view details on neighbors of a mesh access point from a mesh network map, follow these steps:
Step 1  Choose Maps > Site Maps.

Step 2  Click the map name that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3  To view detailed information on mesh links for a mesh access point, click the arrow portion of the access point label. The Access Points page appears.

Step 4  Click the Mesh Links tab.

Note  You can also view mesh link details for neighbors of a selected access point by clicking the View Mesh Neighbors link on the Mesh tab of the access point configuration summary dialog box, which appears when you hover your mouse cursor over an access point on a map.

Note  Signal-to-noise (SNR) appears in the View Mesh Neighbors dialog box.

Note  In addition to listing the current and past neighbors in the dialog box that appears, labels are added to the mesh access points map icons to identify the selected access point, the neighbor access point, and the child access point. Click the clear link of the selected access point to remove the relationship labels from the map.

Note  The drop-down lists at the top of the mesh neighbors page indicate the resolution of the map (100%) displayed and how often the information displayed is updated (every 5 mins). You can modify these default values.

Viewing the Mesh Network Hierarchy

You can view the parent-child relationship of mesh access points within a mesh network in an easily navigable display. You can also filter which access points are displayed in the map view by selecting only access points of interest.

To view the mesh network hierarchy for a selected network, follow these steps:

Step 1  Choose Maps > Site Maps.

Step 2  Click the map name you want to display.

Step 3  Select the AP Mesh Info check box in the left sidebar menu if it is not already selected.

Note  The AP Mesh Info check box is only selectable if mesh access points are present on the map. It must be selected to view the mesh hierarchy.

Step 4  Click the blue arrow to the right of the AP Mesh Info to display the Mesh Parent-Child Hierarchical View.

Step 5  Click the plus (+) sign next to a mesh access point to display its children.
All subordinate mesh access points are displayed when a negative (-) sign appears next to the parent mesh access point entry. For example, the access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*.

### Step 6
Hover your mouse cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 42-11 summarizes the parameters that appear.

The color of the dot also provides a quick reference point of the SNR strength:

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

#### Table 42-11  Bridging Link Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information fetched on</td>
<td>Date and time that information was compiled.</td>
</tr>
<tr>
<td>Link SNR</td>
<td>Link signal-to-noise ratio (SNR).</td>
</tr>
<tr>
<td>Link Type</td>
<td>Hierarchical link relationship.</td>
</tr>
<tr>
<td>SNR Up</td>
<td>Signal-to-noise radio for the uplink (dB).</td>
</tr>
<tr>
<td>SNR Down</td>
<td>Signal-to-noise radio for the downlink (dB).</td>
</tr>
<tr>
<td>PER</td>
<td>The packet error rate for the link.</td>
</tr>
<tr>
<td>Tx Parent Packets</td>
<td>The TX packets to a node while acting as a parent.</td>
</tr>
<tr>
<td>Rx Parent Packets</td>
<td>The RX packets to a node while acting as a parent.</td>
</tr>
<tr>
<td>Time of Last Hello</td>
<td>Date and time of last hello.</td>
</tr>
</tbody>
</table>

---

**Using Mesh Filters to Modify Map Display of Maps and Mesh Links**

In the mesh hierarchical page, you can also define mesh filters to determine which mesh access points display on the map based on hop values as well as what labels display for mesh links.

Mesh access points are filtered by the number of hops between them and their root access point.

To use mesh filtering, follow these steps:

#### Step 1
To modify what label and color displays for a mesh link, follow these steps:

- In the Mesh Parent-Child Hierarchical View, choose an option from the Link Label drop-down list. Options are None, Link SNR, and Packet Error Rate.
- In the Mesh Parent-Child Hierarchical View, choose an option from the Link Color drop-down list to define which parameter (Link SNR or Packet Error Rate) determines the color of the mesh link on the map.
The color of the link provides a quick reference point of the SNR strength or Packet Error Rate. Table 42-17 defines the different link colors.

### Table 42-12 Definition for SNR and Packet Error Rate Link Color

<table>
<thead>
<tr>
<th>Link Color</th>
<th>Link SNR</th>
<th>Packet Error Rate (PER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Represents a SNR above 25 dB (high value)</td>
<td>Represents a PER of one percent (1%) or lower</td>
</tr>
<tr>
<td>Amber</td>
<td>Represents a SNR between 20 and 25 dB (acceptable value)</td>
<td>Represents a PER that is less than ten percent (10%) and greater than one percent (1%)</td>
</tr>
<tr>
<td>Red</td>
<td>Represents a SNR below 20 dB (low value)</td>
<td>Represents a PER that is greater than ten percent (10%)</td>
</tr>
</tbody>
</table>

The Link label and color settings are reflected on the map immediately. You can display both SNR and PER values simultaneously.

### Step 2
To modify which mesh access points display based on the number of hops between them and their parents, do the following:

- a. In the Mesh Parent-Child Hierarchical View, choose the appropriate options from the Quick Selections drop-down list. A description of the options is provided in Table 42-18.

### Table 42-13 Quick Selection Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select only Root APs</td>
<td>Choose this setting if you want the map view to display root access points only.</td>
</tr>
<tr>
<td>Select up to 1st hops</td>
<td>Choose this setting if you want the map view to display 1st hops only.</td>
</tr>
<tr>
<td>Select up to 2nd hops</td>
<td>Choose this setting if you want the map view to display 2nd hops only.</td>
</tr>
<tr>
<td>Select up to 3rd hops</td>
<td>Choose this setting if you want the map view to display 3rd hops only.</td>
</tr>
<tr>
<td>Select up to 4th hops</td>
<td>Choose this setting if you want the map view to display 4th hops only.</td>
</tr>
<tr>
<td>Select All</td>
<td>Select this setting if you want the map view to display all access points.</td>
</tr>
</tbody>
</table>

- b. Click Update Map View to refresh the screen and display the map view with the selected options.

Map view information is retrieved from the Prime Infrastructure database and is updated every 15 minutes.
Monitoring Tags Using Maps

On an Prime Infrastructure map, you can review the name of the access point that generated the signal for a tagged asset, its strength of signal and when the location information was last updated for the asset. This information is displayed by simply hovering the mouse cursor over the asset tag icon on the map.

To enable tag location status on a map, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** Choose Campus > Building > Floor for the applicable mobility services engine and tag.

**Step 3** Select the 802.11 Tags check box in the Floor Settings pane (left), if not already selected.

**Note** Do not click Save Settings unless you want to save changes made to the Floor Settings across all maps.

**Step 4** Hover the mouse cursor over a tag icon (yellow tag) and a summary of its configuration appears in a dialog box.

**Step 5** Click the tag icon to see tag details in a new window.

Using Planning Mode

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location are active.

**Note** Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of access points required that would provide optimum coverage in your network.
Accessing Planning Mode

To access the Planning Mode feature, follow these steps:

**Step 1**  Choose **Maps > Site Maps**.

**Step 2**  Select the desired campus or building from the Name list.

**Step 3**  Click the desired floor area in the Building.

**Step 4**  From the Select a command drop-down list, choose **Planning Mode**.

**Step 5**  Click **Go**.

---

**Note**  Planning mode does not use AP type or Antenna pattern information for calculating the number of access points required. The calculation is based on the access point coverage area or the number of users per access point.

Planning Mode options:

- **Add APs**—Enables you to add access points on a map. See the Using Planning Mode to Calculate Access Point Requirements for details.
- **Delete APs**—Deletes the selected access points.
- **Map Editor**—Opens the Map Editor window. See the Using the Map Editor for more details.
- **Synchronize with Deployment**—Synchronizes your planning mode access points with the current deployment scenario.
- **Generate Proposal**—View a planning summary of the current access points deployment.
- **Planned AP Association Tool**—Allows you to perform add, delete or import an AP Association from an excel or CSV file. Once an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered they get pushed into a standby bucket and get associated when discovered.

**Note**  AP association is subjected to a limitation that AP should not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP and when removed from the floor or outdoor, get positioned to the given floor. One Mac address cannot be put into bucket for multiple floor or outdoor areas.

**Note**  The map synchronizations works only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.

---

**Related Topics**

- Using Planning Mode
- Using Planning Mode to Calculate Access Point Requirements
Using Planning Mode to Calculate Access Point Requirements

Prime Infrastructure planning mode enables you to calculate the number of access points required to cover an area by placing fictitious access points on a map and allowing you to view the coverage area. Based on the throughput specified for each protocol (802.11a/n or 802.11b/g/n), planning mode calculates the total number of access points required to provide optimum coverage in your network. You can calculate the recommended number and location of access points based on the following criteria:

- traffic type active on the network: data or voice traffic or both
- location accuracy requirements
- number of active users
- number of users per square footage

To calculate the recommended number and placement of access points for a given deployment, follow these steps:

**Step 1** Choose Maps > Site Maps.

The Site Map page appears.

**Step 2** Select the appropriate location link from the list that appears.

A color-coded map appears showing placement of all installed elements (access points, clients, tags) and their relative signal strength.

**Step 3** Choose Planning Mode from the Select a command drop-down list (top-right), and click Go. A blank floor map appears.

**Step 4** Click Add APs.

**Step 5** In the page that appears, drag the dashed-line rectangle over the map location for which you want to calculate the recommended access points.

**Note** Adjust the size or placement of the rectangle by selecting the edge of the rectangle and holding down the Ctrl key. Move the mouse as necessary to outline the targeted location. When you use the next-generation maps mode, the rectangle is resizable by dragging on the handles on its edges and corners.

**Step 6** Choose Automatic from the Add APs drop-down list.

**Step 7** Choose the AP Type and the appropriate antenna and protocol for that access point.

**Step 8** Choose the target throughput for the access point.

**Step 9** Select the check box(es) next to the service(s) that is used on the floor. Options are Data/Coverage (default), Voice, Location, and Location with Monitor Mode APs. (see Table 42-19).

**Note** You must select at least one service or an error occurs.

**Note** If you select the Advanced Options check box, two additional access point planning options appear: Demand and Override Coverage per AP. Additionally, a Safety Margin field appears for the Data/Coverage and Voice safety margin options.
### Table 42-14  Definition of Services Option

<table>
<thead>
<tr>
<th>Service Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data/Coverage</strong></td>
<td>Select this check box if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:</td>
</tr>
<tr>
<td><strong>Voice</strong></td>
<td>Select the Voice check box if voice traffic is transmitted on the wireless LAN.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Select this check box to ensure that the recommended access point calculation provides the true location of an element within 10 meters at least 90% of the time.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.</td>
</tr>
</tbody>
</table>

#### Table 42-14 Data/Coverage

<table>
<thead>
<tr>
<th>Band</th>
<th>Path Loss Model (dBm)</th>
<th>Date Rate (Mb/s)</th>
<th>Area (Sq. ft.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>–3.3</td>
<td>10-12</td>
<td>6000</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
<td>15-18</td>
<td>4500</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
<td>10-12</td>
<td>5000</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
<td>15-18</td>
<td>3250</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
<td>5</td>
<td>6500</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
<td>6</td>
<td>4500</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
<td>5</td>
<td>5500</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
<td>6</td>
<td>3500</td>
</tr>
</tbody>
</table>

If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, very safe) of the signal strength threshold for data.

- **Aggressive** = Minimum (–3 dBm)
- **Safe** = Medium (0 dBm)
- **Very Safe** = Maximum (+3 dBm)

If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, very safe, or 7920-enabled) of the signal strength threshold for voice.

- **Aggressive** = Minimum [–78 dBm (802.11a/b/g)]
- **Safe** = Medium [–75 dBm (802.11a/b/g)]
- **Very Safe** = Maximum [–72 dBm (802.11a/b/g)]
- **7920_enabled** = [–72 dBm (802.11a); –67 dBm (802.11b/g)]
### Table 42-15 Definition of Advanced Services

<table>
<thead>
<tr>
<th>Service Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data/Coverage</strong></td>
<td>Select this check box, if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:</td>
</tr>
<tr>
<td>Band</td>
<td>Path Loss Model (dBm)</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
</tr>
<tr>
<td>If you select the Advanced Options check box, you can select the desired safety margin (aggressive, safe, or very safe) of the signal strength threshold for data.</td>
<td></td>
</tr>
<tr>
<td>• Aggressive = Minimum (–3 dBm)</td>
<td></td>
</tr>
<tr>
<td>• Safe = Medium (0 dBm)</td>
<td></td>
</tr>
<tr>
<td>• Very Safe = Maximum (+3 dBm)</td>
<td></td>
</tr>
<tr>
<td><strong>Voice</strong></td>
<td>Select the voice check box if voice traffic is transmitted on the wireless LAN.</td>
</tr>
<tr>
<td>If you select the Advanced Options check box, you can select the desired safety margin (aggressive, safe, very safe or 7920-enabled) of the signal strength threshold for voice.</td>
<td></td>
</tr>
<tr>
<td>• Aggressive = Minimum [–78 dBm (802.11a/b/g)]</td>
<td></td>
</tr>
<tr>
<td>• Safe = Medium [–75 dBm (802.11a/b/g)]</td>
<td></td>
</tr>
<tr>
<td>• Very Safe = Maximum [–72 dBm (802.11a/b/g)]</td>
<td></td>
</tr>
<tr>
<td>7920_enabled = [–72 dBm (802.11a); –67 dBm (802.11b/g)]</td>
<td></td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Select this check box to ensure that the recommended access point calculation provides the true location of an element within 10 meters at least 90% of the time.</td>
</tr>
<tr>
<td>To meet the criteria, access points are collocated within 70 feet of each other in a hexagonal pattern employing staggered and perimeter placement.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.</td>
<td></td>
</tr>
<tr>
<td><strong>Demand</strong></td>
<td>Select this check box if you want to use the total number of users or user ratio per access point as a basis for the access point calculation.</td>
</tr>
</tbody>
</table>
Step 10  Click **Calculate**.

The recommended number of access points given the selected services appears.

**Note**

Recommended calculations assume the need for consistently strong signals unless adjusted downward by the **safety margin** advanced option. In some cases, the recommended number of access points is higher than what is required.

**Note**

Walls are not used or accounted for in planning mode calculations.

Step 11  Click **Apply** to generate a map that shows proposed deployment of the recommended access points in the selected area based on the selected services and parameters.

Step 12  Choose **Generate Proposal** to display a textual and graphical report of the recommended access point number and deployment based on the given input.

### Wireless Map Refresh Options

Prime Infrastructure provides various refresh options for wireless maps:

- **Load**—Refreshes map data from the Prime Infrastructure database on demand.
- **Auto Refresh**—Provides an interval drop-down list to set how often to refresh the map data from the database.
- **Refresh from network**—Refreshes the map status and statistics directly from the controller through an SNMP fetch rather than polled data from the Prime Infrastructure database.

If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points, and an IDS heatmap includes them.

- **Refresh browser**—Refreshes the complete page, or refreshes the map and its status and statistics if you are on a map page.
Understanding RF Heatmap Calculation

A radio frequency heat map is a graphical representation of the strength of the RF signals. Because WLANs are very dynamic and nondeterministic in nature, administrators can never be certain of the coverage at a particular moment. To help combat this challenge, Prime Infrastructure provides a map of your floor plan along with visual cues as to the Wi-Fi coverage of the floor. These maps are called heatmaps because they are similar to the colored maps used to show varying levels of heat in oceanography or geographical sciences. Color is used to show the various levels of signal strength. The different shades in the “heatmap” reflect differing signal strengths.

This color visualization provides a quick view of the current state of coverage (without having to walk around measuring it), the signal strength, and any gaps or “holes” in the WLAN. This enhances the speed and ease with which you support your organization and troubleshoot specific problems.

The RF heatmap calculation is based on an internal grid. Depending on the exact positioning of an obstacle in that grid, the RF heatmap, within a few feet or meters of the obstacle, might or might not account for the obstacle attenuation. The RF prediction heatmaps for access points approximates of the actual RF signal intensity. It takes into account the attenuation of obstacles drawn using the Map Editor but it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions. The thick wall (color-coded orange) with a loss of 13 dB might not be enough to contain the RF signal beyond the walls of the heatmap.

In detail, grid squares partially affected by an obstacle crossing the grid square might or might not incorporate the obstacle attenuation according to the geometry of the access point, obstacle, and grid.

For example, consider a wall crossing one grid square. The midpoint of the grid square is behind the wall from the AP, so the whole grid square is colored with attenuation, including (unfortunately) the top left corner that is actually in front of the wall.

The midpoint of the grid square is on the same side of the wall as the AP, so the whole grid square is not colored with attenuation, including (unfortunately) the bottom right corner that is actually behind the wall from the AP.

Dynamic Heatmap Calculation

The RF heatmap calculation can be static or dynamic. By default, it is dynamic. The main purpose of the dynamic heatmap feature is to recompute the RF heatmaps due to obstacles. The Prime Infrastructure server maintains a current list of all APs’ RSSI strengths. Prime Infrastructure uses neighboring APs’ RSSI strength to modify the RF heatmaps for all APs.

To configure static heatmap calculation, you must disable the dynamic heatmap option in the map properties page.

Drawing Polygon Areas in Wireless Maps

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a polygon-shaped area.

Step 1  Choose Maps > Site Maps.
Step 2  Click the outdoor area, campus, building, or floor you want to edit.
Step 3  From the Select a command drop-down list, choose Map Editor, and click Go.
Chapter 42  Using Wireless Maps

Step 4  On the Map Editor page, click the **Add Perimeter** icon.

Step 5  Enter the name of the area that you are defining, then click **OK**.

A drawing tool appears.

Step 6  Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.
- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

The outlined area must be a closed object to appear highlighted on the map.

Step 7  Click the disk icon to save the newly drawn area.

Step 8  Choose **Command > Exit** to close the window. You return to the original floor plan.

| Note | When you return to the original floor plan view after exiting the map editor, the newly drawn area is not visible; however, it appears in the Planning Model page when you add elements. |

Step 9  Choose **Planning Mode** from the Select a command drop-down list to begin adding elements to the newly defined polygon-shaped area.

---

**Floor View in Wireless Maps**

The main Floor View navigation pane provides access to multiple map functions and includes the following functionality:

- **Zoom In/Zoom Out**—Click the magnifying glass icon with the plus sign (+) to enlarge the map view. Click the magnifying glass icon with the minus sign (-) to decrease the size of the map view.
- **Map Size**—See “Panning and Zooming with Next Generation Maps” in Related Topics.
- **Show Grid**—Click to show or hide the grid that displays distance in feet on the map.
- **RSSI Legend**—Hover your mouse cursor over the RSSI Legend icon to display the RSSI color scheme (ranging from red/-35 dBm to dark blue/-90 dBm).
- **Add Access Points**—Click to open the Add Access Points page. For more information, see “Adding Access Points to a Floor Area” in Related Topics.
- **Remove Access Points**—Click to open the Remove Access Points page. Select the access points that you want to remove and click **OK**.
- **Position Access Points**—Click to open the Position Access Points page.
- **Add Chokepoints**—Click to open the Add Chokepoints page. For more information, see the *Cisco Context-Aware Services Configuration Guide*.
- **Add WiFi TDOA Receivers**—Click to open the Add Wi-Fi TDOA Receivers page. For more information, see the *Cisco Context-Aware Services Configuration Guide*.
- **Auto Refresh**—From the drop-down list, choose the length of time between each system refresh.
- **Refresh from Network**—Click to initiate an immediate refresh of the current data.
- **Planning Mode**—Click to open the Planning Mode window. For more information, see “Using Planning Mode” in Related Topics.
Associating Endpoints with a Site

Endpoint-Site association rules allow you to associate all of the devices on particular subnet to a site, or location, and (optionally) to specify the monitoring data source for the devices on that subnet. This allows you to associate the logical structure of your network with your organizational sites, enabling troubleshooting using Prime Infrastructure’s multi-segment analysis features.

You can specify multiple rules for the same subnet, allowing you to (for example) specify multiple monitoring data sources.

To associate endpoints with a site:

Step 1 Choose Services > Application Visibility & Control > Endpoint Association.
Step 2 Click Add Row to add an Endpoint-Site association rule.
Step 3 Enter the required parameters in the following fields:
  - From the Location Group drop-down list, select an existing campus to associate with this subnet. This field can be used to display the filter and search results.
  - In the Subnet field, enter the routing prefix (and optional Data Source) of the subnetwork to be associated with this site. The entry must be in Classless Inter-Domain Routing notation.
  - From the Data Source drop-down list, select the edge router or NAM monitoring traffic to and from the devices in the specified subnetwork.
Step 4 Click Save.

Viewing Google Earth Maps in Prime Infrastructure

You must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server.

Step 1 Choose Maps > Google Earth. The Google Earth Maps page displays all folders and the number of access points included within each folder.
Step 2 Click Launch for the map you want to view. Google Earth opens in a separate page and displays the location and its access points.
Creating Outdoor Locations using Geographical Coordinates

To group access points together into outdoor locations, use the Latitude/Longitude geographical coordinates for each access point. You first need to create the required access point geographical coordinates, which you can then import into Prime Infrastructure. You can create either of the following file types to provide the coordinates:

- A KML (Google Keyhole Markup Language) File
- A CSV File (Spreadsheet format with comma-separated values)

Related Topics
- Required Geographical Coordinates
- Creating a KML File with Geographical Coordinates
- Creating a CSV File with Geographical Coordinates
- Importing Geographical Coordinates Files into Prime Infrastructure
Creating Outdoor Locations using Geographical Coordinates

Required Geographical Coordinates

You must provide the following geographical information for each access point. You can create the geographical coordinates in Google Earth and then import them into Prime Infrastructure. If you add an AP to a Google Earth map without having the AP associated on a standard map, you will not see a heatmap when you view the AP in Google Earth.

- Longitude (East or West)—Angular distance in degrees relative to Prime Meridian. Values west of Meridian range from –180 to 0 degrees. Values east of Meridian range from 0 to 180 degrees. The default is 0.

  Coordinates in degrees, minutes, seconds, direction:
  - Degrees (–180 to 180)
  - Minutes (0 to 59)
  - Seconds (00.00 to 59.99)
  - Direction—East or West (E, W)

  Decimal format (converted from degrees, minutes, and seconds):
  - Longitude can range from –179.59.59.99 W to 179.59.59.99 E

- Latitude (North or South)—Angular distance in degrees relative to the Equator. Values south of the Equator range from –90 to 0 degrees. Values north of the Equator range from 0 to 90 degrees. The default is 0.

  Coordinates in degrees, minutes, seconds, direction:
  - Degrees (–90 to 90)
  - Minutes (0 to 59)
  - Seconds (00.00 to 59.99)
  - Direction—North or South (N, S)

  Decimal format (converted from degrees, minutes, and seconds):
  - Latitude can range from –89.59.59.99 S to 89.59.59.99 N

- Altitude—Height or distance of the access point from the surface of the earth in meters. If not provided, value defaults to 0. Values range from 0 to 99999.

- Tilt—Values range from 0 to 90 degrees (cannot be negative). A tilt value of 0 degrees indicates viewing from directly above the access point. A tilt value of 90 degrees indicates viewing along the horizon. Values range from 0 to 90. The default azimuth angle is 0.

- Range—Distance in meters from the point specified by longitude and latitude to the point where the access point is being viewed (the Look At position) (camera range above sea level). Values range from 0 to 999999.

- Heading—Compass direction in degrees. The default is 0 (North). Values range from 0 to ±180 degrees.

- Altitude Mode—Indicates how the <altitude> specified for the Look At point is interpreted.
  - Clamped to ground—Ignores the <altitude> specification and places the Look At position on the ground. This is the default.
  - Relative to ground—Interprets the <altitude> as a value in meters above the ground.
  - Absolute—Interprets the <altitude> as a value in meters above sea level.

- Extend to ground—Indicates whether or not the access point is attached to a mast.
Creating Outdoor Locations using Geographical Coordinates

Creating a KML File with Geographical Coordinates

You can create the geographical coordinates in Google Earth and then import them into Prime Infrastructure. You can create either a folder or individual placemarks. Creating a folder helps group all the Placemarks into a single folder and allows you to save the folder as a single KML (a.k.a. XML) file. KML is a file format used to display geographic data in Google Earth. If you create individual Placemarks, you must save each Placemark individually.

Using a KML file, folders can be created hierarchically to any depth. For example, you can create folders and placemarks organized by country, city, state, zip. In CSV files, there is one level of hierarchy only.

Step 1
Launch Google Earth.

Step 2
In the Places page on the left sidebar menu, choose My Places or Temporary Places.

Step 3
Right-click Temporary Places and select Add > Folder from the drop-down lists.

Step 4
Enter the required information.
If you specify View coordinates (latitude, longitude, range, heading, and tilt), this information is used to “fly” or advance to the correct location when Google Earth is first loaded. If you do not specify View coordinates, the latitude and longitude information is derived using the minimum and maximum latitude and longitude of all access points within the specified group or folder.

Step 5
Click OK.

After the folder is created, you can select it from the Places page to create Placemarks.

Related Topics
- Creating Placemarks for KML Files
- Required Geographical Coordinates

Creating Placemarks for KML Files

To create Placemarks, follow these steps:

Step 1
Launch Google Earth.

Step 2
In the Places page on the left sidebar, select My Places or Temporary Places.

Step 3
Select the folder that you previously created.

Step 4
Right-click your created folder and select Add > Placemark from the drop-down lists.

Step 5
Complete the required fields. For more information regarding Google Earth, see to the Google Earth online help.

The Placemark name must contain the name, MAC address (the radio MAC not Ethernet MAC), or IP address of the appropriate access point.

Step 6
Click Snapshot current view or click Reset to return the coordinates to the original settings.

Step 7
Click OK.

Step 8
Repeat these steps for all placemarks you want to add.
Creating Outdoor Locations using Geographical Coordinates

**Step 9**

When all placemarks are created, save the folder as a .kmz file (KML Zip file) or as a .kml file. You can import both .kmz and .kml files into Prime Infrastructure.

---

**Related Topic**

Required Geographical Coordinates

---

Creating a CSV File with Geographical Coordinates

You can create a CSV file that contains the required access point geographical coordinates, and then import the CSV file into Prime Infrastructure.

**Step 1**

Using a text editor, create a new file that provides the necessary fields, separated by commas, as described in Table 42-16.

**Table 42-16 Sample Fields for Geographical Coordinates CSV File**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value Required/Optional</th>
<th>Max Length/MIN</th>
<th>Permitted Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>FolderName</td>
<td>“Value Optional”</td>
<td>Max Length: 32</td>
<td></td>
</tr>
<tr>
<td>FolderState</td>
<td>“Value Optional”</td>
<td></td>
<td>Permitted Values: true/false</td>
</tr>
<tr>
<td>FolderLongitude</td>
<td>“Value Optional”</td>
<td>Range: 0 to ±180</td>
<td></td>
</tr>
<tr>
<td>FolderLatitude</td>
<td>“Value Optional”</td>
<td>Range: 0 to ±90</td>
<td></td>
</tr>
<tr>
<td>FolderAltitude</td>
<td>“Value Optional”</td>
<td>Range: 0 to 99999</td>
<td></td>
</tr>
<tr>
<td>FolderRange</td>
<td>“Value Optional”</td>
<td>Range: 0 to 99999</td>
<td></td>
</tr>
<tr>
<td>FolderTilt</td>
<td>“Value Optional”</td>
<td>Range: 0 to 90</td>
<td></td>
</tr>
<tr>
<td>FolderHeading</td>
<td>“Value Optional”</td>
<td>Range: 0 to ±180</td>
<td></td>
</tr>
<tr>
<td>FolderGeoAddress</td>
<td>“Value Optional”</td>
<td>Max Length: 128</td>
<td></td>
</tr>
<tr>
<td>FolderGeoCity</td>
<td>“Value Optional”</td>
<td>Max Length: 64</td>
<td></td>
</tr>
<tr>
<td>FolderGeoState</td>
<td>“Value Optional”</td>
<td>Max Length: 40</td>
<td></td>
</tr>
<tr>
<td>FolderGeoZip</td>
<td>“Value Optional”</td>
<td>Max Length: 12</td>
<td></td>
</tr>
<tr>
<td>FolderGeoCountry</td>
<td>“Value Optional”</td>
<td>Max Length: 64</td>
<td></td>
</tr>
<tr>
<td>AP_Name</td>
<td>“Value Required”</td>
<td>Max Length: 32</td>
<td></td>
</tr>
<tr>
<td>AP_Longitude</td>
<td>“Value Required”</td>
<td>Range: 0 to ±180</td>
<td></td>
</tr>
<tr>
<td>AP_Latitude</td>
<td>“Value Required”</td>
<td>Range: 0 to ±90</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

Save the file with a .csv file extension.

---

**Related Topic**

Required Geographical Coordinates
Importing Geographical Coordinates Files into Prime Infrastructure

To group access points together into outdoor locations, use the Latitude/Longitude geographical coordinates for each access point. You first need to create the required access point geographical coordinates, which you can then import into Prime Infrastructure. You can import either a Google KML or a CSV file containing access point geographical coordinates into Prime Infrastructure.

**Step 1** Choose Maps > Google Earth.

**Step 2** From the Select a command drop-down list, choose Import Google KML or Import CSV, then click Go.

**Step 3** Navigate to the .kml, .kmz, or .csv file on your computer, then click Next.

The input file is parsed and validated for the following:

- Access points specified in the uploaded file are validated (the specified access points must be available within Prime Infrastructure).
- Range validations are performed for tilt, heading, range, and other geographical coordinates fields. If longitude and latitude are provided, range validations are performed; if not, the value is defaulted to 0.

**Step 4** After the files pass all validation checks, review the file details and click Save.

If the uploaded information was previously saved, the information is overwritten as follows:

- If the folder was uploaded previously, the coordinates are updated for the folder.
- If access points were uploaded previously, the coordinates are updated for the access points.
- Existing access points in the folder are not removed.
- New folders are created as needed and access points are placed accordingly.

Adding Google Earth Location Launch Points to Access Point Pages

You can expand the number of Google Earth Location launch points within Prime Infrastructure by adding launch points to the Access Point summary and detail pages.

**Step 1** Choose Monitor > Wireless Technologies > Access Point Radios.

**Step 2** In the Access Point summary page, click the Edit View link next to page heading.

**Step 3** In the Edit View page, highlight Google Earth Location in the left-hand column, then click Show.

The Google Earth Location column heading moves into the View Information column.

**Step 4** To change the display order of the columns, highlight the Google Earth Location entry and click the Up and Down buttons as needed, then click Submit.

You are returned to the Access Points summary page, and a Google Earth launch link appears. The launch link also appears in the general summary page of the Access Points details page (Monitor > Wireless Technologies > Access Point Radios > AP Name).
Configuring Google Earth Settings for Access Points

You can configure access point settings for the Google Earth Maps feature:

**Step 1** Choose Maps > Google Earth.

**Step 2** Configure the following parameters:

- **Refresh Settings**—Select the Refresh from Network check box to enable on-demand refresh. This option is applied only once and then disabled. Based on the number of access points in your network, the refresh can take a long period of time.

- **Layers**—Layer filters for access points, access point heat maps, and access point mesh information can be selected and saved. Select the check box to activate the applicable layer and click > to open the filter page. These settings apply when Google Earth sends the request for the next refresh.
  - **Access Points**—From the AP Filter drop-down list, choose to display channels, Tx power level, coverage holes, MAC addresses, names, controller IP, utilization, profiles, or clients.
    
    If the access point layer is not checked, no data is returned, and an error message is returned to Google Earth as a Placemark without an icon.
  
  - **AP Heatmap**—From the Protocol drop-down list, choose 802.11a/n, 802.11b/g/n, 802.11a/n & 802.11b/g/n, or None. Select the cutoff from the RSSI Cutoff drop-down list (-60 to -90 dBm).
    
    If you chose both 802.11a/n and 802.11b/g/n, the heat maps are generated for both and overlaid on top of each other. The order cannot be defined. To prevent this overlay, you must turn off individual overlay in Google Earth or change it in the Google Earth Settings in Prime Infrastructure.
  
  - **AP Mesh Info**—Choose Link SNR, Packet Error Rate, or none. Choose Link SNR or Packet Error Rate from the Link Color drop-down list. When you select AP Mesh Info, Mesh Links are also automatically shown.

**Step 3** Click Save Settings to confirm these changes or Cancel to close the page without saving the changes.

---

Editing Wireless Maps

Editing Floors

Editing Wireless Maps

Follow these steps to use the wireless map editor:
Step 1  Choose Maps > Site Maps.

Step 2  Select the desired campus, building and floor area.

Step 3  Click the desired floor area. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.

Step 4  From the Select a command drop-down list, choose Map Editor, and click Go. The Map Editor page appears.

Make sure that the floor plan images are properly scaled so that all white space outside of the external walls is removed. To make sure that floor dimensions are accurate, click the compass tool.

Step 5  Position the reference length. The Scale menu appears with the line length supplied. Enter the dimensions (width and height) of the reference length, then click OK.

Step 6  Determine the propagation pattern from the Antenna Mode drop-down list.

Step 7  Make antenna adjustments by sliding the antenna orientation bar to the desired degree of direction.

Step 8  Choose the desired access point.

Step 9  Click Save.

**Location Accuracy**

Prime Infrastructure allows you to check the location quality and the ability of a given location to meet the location specification (10 m, 90%) based on data points gathered during a physical inspection and calibration.

**Related Topics**

- Viewing Location Accuracy and Readiness
- Inspecting Location Quality Using Calibration Data
- Viewing VoWLAN Readiness

**Viewing Location Accuracy and Readiness**

You can configure Prime Infrastructure to verify the existing access point deployment to estimate the true location of a client, rogue client, rogue access point, or tag within 10 meters at least 90% of the time. The location readiness calculation is based on the number and placement of access points.

The Inspect Location Readiness feature is a distance-based predictive tool that can point out problem areas with access point placement.

To access the Inspect Location Readiness tool, follow these steps:

Step 1  Choose Maps > Site Maps.

Step 2  Click the applicable floor area name to view the map.

If RSSI is not displayed, you can enable AP Heatmaps by selecting the AP Heatmaps check box on the left sidebar menu.
If clients, tags, and access points are not displayed, verify that their respective check boxes are selected on the left sidebar menu. Licenses for both clients and tags must be purchased for each to be tracked.

**Step 3** From the **Select a command** drop-down list, choose **Inspect Location Readiness**.

**Step 4** Click **Go**.

A color-coded map appears showing those areas that meet (indicated by Yes) and do not meet (indicated by No) the ten meter, 90% location specification.

---

**Inspecting Location Quality Using Calibration Data**

After completing a calibration model based on data points generated during a physical tour of the area, you can inspect the location quality of the access points based on calibration.

**Step 1** Choose **Maps > Site Maps**.

**Step 2** Choose **RF Calibration Model** from the Select a command list, then click **Go**.

A list of calibration models appears.

**Step 3** Click the desired calibration model.

**Step 4** Click the **Inspect Location Quality** link found under the Calibration Floors heading.

Prime Infrastructure displays a color-coded map noting percentage of location errors. You can modify the distance selected to see the effect on the location errors.

---

**Viewing VoWLAN Readiness**

The VoWLAN Readiness (voice readiness) Tool allows you to check the RF coverage to determine if it is sufficient for your voice needs. This tool verifies RSSI levels after access points have been installed.

**Step 1** Choose **Maps > Site Maps**.

**Step 2** Click the applicable floor area name.

**Step 3** From the **Select a command** drop-down list, choose **Inspect VoWLAN Readiness**.

**Step 4** Choose the applicable **Band**, **AP Transmit Power**, and **Client** parameters from the drop-down lists.

By default, the region map displays the b/g/n band for Cisco Phone-based RSSI threshold. The new settings cannot be saved.

Depending on the selected client, the following RSSI values might not be editable:

- **Cisco Phone**—RSSI values are not editable.
- **Custom**—RSSI values are editable with the following ranges:
  - Low threshold between -95dBm to -45dBm
  - High threshold between -90dBm to -40dBm

The following color schemes indicate whether or not the area is voice ready:

- **Green**—Yes
Chapter 42  Using Wireless Maps

Location Accuracy

- Yellow—Marginal
- Red—No

The accuracy of the Green/Yellow/Red regions depends on the RF environment and whether or not the floor is calibrated. If the floor is calibrated, the accuracy of the regions is enhanced.

---

Using Chokepoints to Enhance Tag Location Reporting

Adding Wi-Fi TDOA Receivers

Defining Inclusion Regions on Floors

To further refine locations on a floor, you can define the areas that are included (inclusion areas) and those areas that are not included (exclusion areas). For example, you might want to exclude areas such as an atrium or stairwell within a building, but include a work area (such as cubicles, labs, or manufacturing floors).

By default, Prime Infrastructure defines an inclusion region for each newly added floor. When you define a new inclusion region, any previously defined inclusion region is automatically removed. An inclusion region is indicated by a solid aqua line outlining the region.

To define an inclusion area, follow these steps:

Step 1  Choose Maps > Site Maps.
Step 2  Click the name of the appropriate floor area.
Step 3  From the Select a command drop-down list, choose Map Editor, then click Go.
Step 4  On the map, click the aqua box on the toolbar.
Step 5  Click OK in the message box that appears. A drawing icon appears to outline the inclusion area.
Step 6  To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.
Step 7  Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.
Step 8  Repeat Step 7 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.
Step 9  Choose Save from the Command menu or click the disk icon to save the inclusion region.
Step 10 To return to the floor map to enable inclusion regions on heatmaps, choose Exit from the Command menu.
Step 11  Select the Location Regions check box if it is not already selected. To apply the changes to all floor maps, click Save settings.
Step 12 To resynchronize Prime Infrastructure and MSE databases, choose Services > Synchronize Services. If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 13 In the Synchronize page, choose Network Designs from the Synchronize drop-down list, then click Synchronize. You can confirm that the synchronization is successful by viewing two green arrows in the Sync Status column.

Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Defining Exclusion Regions on Floors

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas). For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Step 1 Choose Maps > Site Maps.
Step 2 Click the name of the appropriate floor area.
Step 3 From the Select a command drop-down list, choose Map Editor.
Step 4 Click Go.
Step 5 On the map, click the purple box on the toolbar.
Step 6 Click OK in the message box that appears. A drawing icon appears to outline the exclusion area.
Step 7 To begin defining the exclusion area, move the drawing icon to the starting point on the map, and click once.
Step 8 Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.
Step 9 Repeat Step 8 until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.
Step 10 To define additional exclusion regions, repeat Step 5 to Step 9.
Step 11 When all exclusion areas are defined, choose Save from the Command menu or click the disk icon on the toolbar to save the exclusion region.
Step 12 To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Then click the X icon on the toolbar.
Step 13 To return to the floor map to enable exclusion regions on heatmaps, choose Exit from the Command menu.
Step 14 Select the Location Regions check box if it is not already selected, click Save settings, and close the Layers configuration page when complete.
Step 15 To resynchronize Prime Infrastructure and location databases, choose Services > Synchronize Services.
Step 16 In the Synchronize page, choose Network Designs from the Synchronize drop-down list, then click Synchronize.
Chapter 42      Using Wireless Maps

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Defining a Rail Line on a Floor

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear.

Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority). The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

Rail line configurations do not apply to tags.

Step 1  Choose Maps > Site Maps.

Step 2  Click the name of the appropriate floor area.

Step 3  Choose Map Editor from the Select a command drop-down list.

Step 4  Click Go.

Step 5  In the map, click the rail icon (to the right of the purple exclusion icon) on the toolbar.

Step 6  Enter a snap-width (feet or meters) for the rail and then click OK. A drawing icon appears.

Step 7  Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 8  Click the drawing icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

Step 9  To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Then, click the X icon on the toolbar.

Step 10  To return to the floor map to enable rails on heatmaps, choose Exit from the Command menu.

Step 11  On the floor map, choose the Layers drop-down list.

Step 12  Select the Rails check box if it is not already selected, then click Save settings.

Step 13  To resynchronize Prime Infrastructure and mobility services engine, choose Services > Synchronize Services.

Step 14  In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Using Maps to Monitor Your Network
Monitoring Mesh Networks Using Maps

Prime Infrastructure allows you to access and view details for the following elements from a mesh network map:

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

Monitoring Mesh Link Statistics Using Maps

You can view the signal-to-noise ratio (SNR) for a specific mesh network link, view the number of packets transmitted and received on that link, and initiate a link test in the Maps > Wireless Maps > Site Maps page.

To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the map name that corresponds to the outdoor area, campus, building, or floor you want to monitor.

**Step 3** From the left sidebar menu, click the arrow to the right of AP Mesh Info. The Mesh Filter dialog box appears.

**Step 4** Move the cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent.

The color of the dot provides a quick-reference indicator of the SNR strength, as follows:

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

**Step 5** Click on a link test. You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.

The link test takes 30 seconds to complete.

**Step 6** To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. The following graphs are displayed for the link:

- SNR Up—Plots the RSSI values of the neighbor from the perspective of the access point.
- SNR Down—Plots the RSSI values that the neighbor reports to the access point.
- Link SNR—Plots a weighed and filtered measurement based on the SNR Up value.
- The Adjusted Link Metric—Plots the value used to determine the least cost path to the root access point. This value represents the ease of getting the rooftop access point and accounts for the number of hops. The lower the ease value, the less likely the path is used.
- The Unadjusted Link Metric—Plots the least cost path to get to the root access point unadjusted by the number of hops. The higher the value for the unadjusted link, the better the path.
Monitoring Mesh Access Points Using Maps

You can view summary information for a mesh access point from a mesh network map. This information is in addition to the information shown for all access points (MAC address, access point model, controller IP address, location, height of access point, access point uptime, and LWAPP uptime).

To view summary and detailed configuration information for a mesh access point from a mesh network map, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the map name that corresponds to the outdoor area, campus, building, or floor location of the access point you want to monitor.

**Step 3** To view summary configuration information for an access point, hover your mouse cursor over the access point that you want to monitor. A dialog box appears with configuration information for the selected access point.

**Step 4** To view detailed configuration information for an access point, double-click the access point appearing on the map. The configuration details for the access point appear.

If the access point has an IP address, a Run Ping Test link is also visible at the bottom of the mesh access point dialog box.

**Related Topic**

- Viewing Mesh Access Point Configuration Details

Viewing Mesh Access Point Configuration Details

To view detailed configuration information for a mesh access point from a mesh network map, follow these steps:

**Step 1** Choose Maps > Site Maps.

**Step 2** Click the map name that corresponds to the outdoor area, campus, building, or floor location of the access point you want to monitor.

**Step 3** Double-click the access point for which you want to view detailed configuration information.

**Step 4** Click any of the following tabs to get the required information:

- **General**—Displays the overall configuration of the mesh access point such as the AP name, MAC address, AP Up time, associated controllers (registered and primary) operational status, and software version.
  The software version for mesh access points is appended with the letter *m* and the word *mesh* appears in parentheses.

- **Interface**—Displays configuration details for the interfaces supported on the mesh access point. Interface options are radio and Ethernet.

- **Mesh Links**—Displays parent and neighbor details (name, MAC address, packet error rate, and link details) for the mesh access point. You can also initiate link tests from this page.
- **Mesh Statistics**—Displays details on the bridging, queue, and security statistics for the mesh access point.

**Related Topic**
- **Monitoring Mesh Access Point Neighbors Using Maps**

### Monitoring Mesh Access Point Neighbors Using Maps

To view details on neighbors of a mesh access point from a mesh network map, follow these steps:

**Step 1** Choose **Maps > Site Maps**.

**Step 2** Click the map name that corresponds to the outdoor area, campus, building, or floor you want to monitor.

**Step 3** To view detailed information on mesh links for a mesh access point, click the arrow portion of the access point label. The Access Points page appears.

**Step 4** Click the **Mesh Links** tab.

**Step 5** To view mesh link details for neighbors of a selected access point, click **View Mesh Neighbors** on the Mesh tab of the access point configuration summary dialog box, which appears when you hover your mouse cursor over an access point on a map.

Signal-to-noise (SNR) appears in the View Mesh Neighbors dialog box.

Labels identify the selected access point, the neighbor access point, and the child access point.

**Step 6** To remove the relationship labels from the map, click the **clear** link of the selected access point.

The drop-down lists at the top of the mesh neighbors page indicate the resolution of the map (100%) displayed and how often the information displayed is updated (every 5 mins).

### Viewing the Mesh Network Hierarchy Using Maps

You can view parent-child relationship of mesh access points within a mesh network. You can also filter which access points are displayed in the map view by selecting only access points of interest.

To view the mesh network hierarchy for a selected network, follow these steps:

**Step 1** Choose **Maps > Site Maps**.

**Step 2** Click the map name you want to display.

**Step 3** Select the **AP Mesh Info** check box if it is not already selected.

The AP Mesh Info check box is only selectable if mesh access points are present on the map.

**Step 4** Click the blue arrow to the right of the AP Mesh Info to display the Mesh Parent-Child Hierarchical View.

**Step 5** Click the **plus (+)** sign next to a mesh access point to display its children.

All subordinate mesh access points are displayed when a negative (-) sign appears next to the parent mesh access point entry. For example, the access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*. 
Step 6
Hover your mouse cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent.

The color of the dot provides a quick reference point of the SNR strength:

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

Using Mesh Filters to Modify Map Display of Maps and Mesh Links

In the mesh hierarchical page, you can define mesh filters to determine which mesh access points appear on the map. Mesh access points are filtered by the number of hops between them and their root access point.

Prime Infrastructure updates map view information every 15 minutes.

To use mesh filtering, follow these steps in the Mesh Parent-Child Hierarchical View:

Step 1
To modify what label and color displays for a mesh link, select an option from the Link Label drop-down list.

Step 2
To choose which parameter determines the color of the mesh link on the map, choose an option from the Link Color drop-down list.

Step 3
To modify which mesh access points are displayed based on the number of hops between them and their parents, choose the appropriate options from the Quick Selections drop-down list.

Step 4
A description of the options is provided in Table 42-18.

Step 5
Click Update Map View to refresh the screen and display the map view with the selected options.

For a child access point to be visible, the parent access point to root access point must be selected.

Related Topics
- SNR and Packet Error Rate Link Colors
- Quick Selection Options

SNR and Packet Error Rate Link Colors

The color of the SNR and Packet Error Rate link provides a quick reference point of the SNR strength as described in Table 42-17.
Using Maps to Monitor Your Network

Chapter 42  Using Wireless Maps

Using Maps to Monitor Your Network

Quick Selection Options

To specify which mesh access points are displayed based on the number of hops between them and their parents, select any of the Quick Selections options described in Table 42-18.

Table 42-17 Definition for SNR and Packet Error Rate Link Color

<table>
<thead>
<tr>
<th>Link Color</th>
<th>Link SNR</th>
<th>Packet Error Rate (PER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Represents a SNR above 25 dB (high value)</td>
<td>Represents a PER of one percent (1%) or lower</td>
</tr>
<tr>
<td>Amber</td>
<td>Represents a SNR between 20 and 25 dB (acceptable value)</td>
<td>Represents a PER that is less than ten percent (10%) and greater than one percent (1%)</td>
</tr>
<tr>
<td>Red</td>
<td>Represents a SNR below 20 dB (low value)</td>
<td>Represents a PER that is greater than ten percent (10%)</td>
</tr>
</tbody>
</table>

Quick Selection Options

To specify which mesh access points are displayed based on the number of hops between them and their parents, select any of the Quick Selections options described in Table 42-18.

Table 42-18 Quick Selection Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select only Root APs</td>
<td>Choose this setting if you want the map view to display root access points only.</td>
</tr>
<tr>
<td>Select up to 1st hops</td>
<td>Choose this setting if you want the map view to display 1st hops only.</td>
</tr>
<tr>
<td>Select up to 2nd hops</td>
<td>Choose this setting if you want the map view to display 2nd hops only.</td>
</tr>
<tr>
<td>Select up to 3rd hops</td>
<td>Choose this setting if you want the map view to display 3rd hops only.</td>
</tr>
<tr>
<td>Select up to 4th hops</td>
<td>Choose this setting if you want the map view to display 4th hops only.</td>
</tr>
<tr>
<td>Select All</td>
<td>Select this setting if you want the map view to display all access points.</td>
</tr>
</tbody>
</table>

Monitoring Tags Using Maps

When you enable tag location status on a map, you can review the name of the access point that generated the signal for a tagged asset, its strength of signal and when the location information was last updated for the asset. To display this information, hover your cursor over the asset tag icon on the map.

Step 1  Choose Maps > Site Maps.
Step 2  Choose Campus > Building > Floor for the applicable mobility services engine and tag.
Step 3  Select the 802.11 Tags check box in the Floor Settings pane (left), if not already selected.
Do not click Save Settings unless you want to save changes made to the Floor Settings across all maps.
Using Maps to Plan Your Network Design

**Using Planning Mode**

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location are active.

Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of access points required that would provide optimum coverage in your network.

Planning mode does not use AP type or Antenna pattern information for calculating the number of access points required. The calculation is based on the access point coverage area or the number of users per access point.

**Step 1** Choose Maps > Site Maps.

**Step 2** Select the desired campus or building.

**Step 3** Click the desired floor area in the Building.

**Step 4** From the Select a command drop-down list, choose **Planning Mode**.

**Step 5** Click Go.

**Step 6** Select a planning mode option

The Planned AP Association Tool allows you to add, delete, or import an AP Association from an excel or CSV file. After an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered, it is placed in a standby bucket and is associated after it is discovered.

AP association requires than the AP does not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP and when removed from the floor or outdoor, is positioned on the specified floor. One MAC address cannot be used for multiple floor or outdoor areas.

The map synchronization works only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.
Using Planning Mode to Calculate Access Point Requirements

Prime Infrastructure planning mode enables you to calculate the number of access points required to cover an area by placing fictitious access points on a map and viewing the coverage area. Based on the throughput specified for each protocol (802.11a/n or 802.11b/g/n), planning mode calculates the total number of access points required to provide optimum coverage in your network. You can calculate the recommended number and location of access points based on the following criteria:

- Traffic type active on the network: data or voice traffic or both
- Location accuracy requirements
- Number of active users
- Number of users per square footage

**Step 1** Choose **Maps > Site Maps**.

**Step 2** Select the desired campus or building.

**Step 3** Click the desired floor area in the Building.

A color-coded map appears showing all elements (access points, clients, tags) and their relative signal strength.

**Step 4** Choose **Planning Mode** from the Select a command drop-down list (top-right), then click **Go**. A blank floor map appears.

**Step 5** Click **Add APs**.

**Step 6** In the page that appears, drag the dashed-line rectangle over the map in the location for which you want to calculate the recommended access points.

Adjust the size or placement of the rectangle by selecting the edge of the rectangle and holding down the **Ctrl** key. The rectangle is resizable by dragging on the handles on its edges and corners.

**Step 7** From the Add APs drop-down list, choose **Automatic**.

**Step 8** Choose the **AP Type** and the appropriate antenna and protocol for the selected access point.

**Step 9** Choose the target throughput for the access point.

**Step 10** Select the check box(es) next to the service(s) used on the floor. You must select at least one service.

**Step 11** Select the **Advanced Options** check box to select the following access point planning options:

- Demand and Override Coverage per AP.
- Safety Margin (for the Data/Coverage and Voice safety margin options)

**Step 12** Click **Calculate**.

The recommended number of access points given the selected services appears. Recommended calculations assume the need for consistently strong signals unless adjusted downward by the safety margin advanced option. In some cases, the recommended number of access points is higher than what is required.

Walls are not used or accounted for in planning mode calculations.

**Step 13** Click **Apply** to generate a map that shows proposed deployment of the recommended access points in the selected area based on the selected services and parameters.

**Step 14** Choose **Generate Proposal** to display a textual and graphical report of the recommended access point number and deployment based on the given input.
Services Options for Planning Mode

Table 42-19 describes the access point planning options.

Table 42-19 Definition of Services Option for Planning Mode

<table>
<thead>
<tr>
<th>Service Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data/Coverage</td>
<td>Select this check box if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:</td>
</tr>
<tr>
<td>Band</td>
<td>Path Loss Model (dBm)</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
</tr>
</tbody>
</table>

If you select the Advanced Options check box, you can select the desired safety margin (aggressive, safe, or very safe) of the signal strength threshold for data.

- Aggressive = Minimum (–3 dBm)
- Safe = Medium (0 dBm)
- Very Safe = Maximum (+3 dBm)

Voice

Select the Voice check box if voice traffic is transmitted on the wireless LAN.

If you select the Advanced Options check box, you can select the desired safety margin (aggressive, safe, very safe or 7920-enabled) of the signal strength threshold for voice.

- Aggressive = Minimum [–78 dBm (802.11a/b/g)]
- Safe = Medium [–75 dBm (802.11a/b/g)]
- Very Safe = Maximum [–72 dBm (802.11a/b/g)]
- 7920_enabled = [–72 dBm (802.11a); –67 dBm (802.11b/g)]

Location

Select this check box to ensure that the recommended access point calculation provides the true location of an element within 10 meters at least 90% of the time.

To meet the criteria, access points are collocated within 70 feet of each other in a hexagonal pattern employing staggered and perimeter placement.

Note Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.
### Table 42-20  Definition of Advanced Services

<table>
<thead>
<tr>
<th>Service Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data/Coverage</strong></td>
<td>Select this check box, if data traffic is transmitted on the wireless LAN. The following densities are used depending on the band and data rates:</td>
</tr>
<tr>
<td>Band</td>
<td>Path Loss Model (dBm)</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11a</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.3</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
</tr>
<tr>
<td>802.11bg</td>
<td>–3.5</td>
</tr>
</tbody>
</table>

If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, or very safe) of the signal strength threshold for data.

- Aggressive = Minimum (–3 dBm)
- Safe = Medium (0 dBm)
- Very Safe = Maximum (+3 dBm)

<table>
<thead>
<tr>
<th>Voice</th>
<th>Select the voice check box if voice traffic is transmitted on the wireless LAN.</th>
</tr>
</thead>
</table>

If you select the **Advanced Options** check box, you can select the desired safety margin (aggressive, safe, very safe or 7920-enabled) of the signal strength threshold for voice.

- Aggressive = Minimum [–78 dBm (802.11a/b/g)]
- Safe = Medium [–75 dBm (802.11a/b/g)]
- Very Safe = Maximum [–72 dBm (802.11a/b/g)]
- 7920_enabled = [–72 dBm (802.11a); –67 dBm (802.11b/g)]

<table>
<thead>
<tr>
<th>Location</th>
<th>Select this check box to ensure that the recommended access point calculation provides the true location of an element within 10 meters at least 90% of the time.</th>
</tr>
</thead>
</table>

To meet the criteria, access points are collocated within 70 feet of each other in a hexagonal pattern employing staggered and perimeter placement.

**Note**: Each service option includes all services that are listed above it. For example, if you select the Location check box, the calculation considers data/coverage, voice, and location in determining the optimum number of access points required.

<table>
<thead>
<tr>
<th>Demand</th>
<th>Select this check box if you want to use the total number of users or user ratio per access point as a basis for the access point calculation.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Override Coverage per AP</th>
<th>Select this check box if you want to specify square foot coverage as the basis for access point coverage.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Safety Margin</th>
<th>Select this check box to qualify relative signal strength requirements for data and voice service in the access point calculation. Options are: Aggressive, Safe, Very Safe, and 7920-enabled (voice only). Select <strong>Aggressive</strong> to require minimal signal strength requirements in the calculation and <strong>Very Safe</strong> to request the highest signal strength.</th>
</tr>
</thead>
</table>
Network Design

A network design is a representation within Prime Infrastructure of the physical placement of access points throughout your facilities. A hierarchy of a single campus, the buildings that comprise that campus, and the floors of each building constitute a single network design.

Designing a Network

After access points have been installed and have joined a controller, and you’ve configured Prime Infrastructure to manage the controllers, you can create a network design.

The location appliance must be set to poll the controllers in that network, as well as be configured to synchronize with that specific network design, to track devices in that environment. The concept and steps to perform synchronization between Prime Infrastructure and the mobility service engine are explained in the Cisco 3350 Mobility Services Engine Configuration Guide.

Step 1 Log in to Prime Infrastructure with SuperUser, Admin, or ConfigManager access privileges.
Step 2 Choose Maps > Site Maps.
Step 3 Create a new Campus and/ or building as explained in XXX <Add xref.>
Step 4 Create a new floor area.
Step 5 Select the access points to be placed on the specific floor map.
   Each access point you add to the floor map is represented by a gray circle (differentiated by access point name or MAC address) and is lined up in the upper left part of the floor map.
Step 6 Drag each access point to the appropriate location. (Access points turn blue when you click them to relocate them.) The small black arrow at the side of each access point represents Side A of each access point, and each arrow of the access point must correspond with the direction in which the access points were installed. (Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio.)
Step 7 To adjust an access point’s directional arrow, choose the appropriate orientation on the Antenna Angle drop-down list.
   Access point placement and direction must directly reflect the actual access point deployment or the system cannot pinpoint the device location.
Step 8 Click Save when you are finished placing and adjusting each direction of the access point.
Step 9 Repeat these steps to create additional campuses, buildings, and floors until each device location is properly detailed in the network design.

Importing or Exporting WLSE Map Data

When you convert an access point from autonomous to CAPWAP and from the WLSE to Prime Infrastructure, you must manually re-enter the access point information in Prime Infrastructure. This can be a time-consuming step. To convert access point information more quickly, you can export the information about access points from WLSE and import it into Prime Infrastructure.

Prime Infrastructure supports importing access point information from a .tar file only.
Troubleshooting Voice RF Coverage Issues

For more information on the WLSE data export functionality (WLSE version 2.15), see http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp.

Step 1  Choose Maps > Site Maps.
Step 2  Choose Properties from the Select a command drop-down list, then click Go.
Step 3  In the Export/Import AP/LS/SP Placement, click Browse to select the file to import.
Step 4  Find and select the .tar file to import, then click Open.
Step 5  Click Import.

Prime Infrastructure uploads the file and temporarily saves it into a local directory while it is being processed. If the file contains data that cannot be processed, Prime Infrastructure prompts you to correct the problem and retry. After the file has been loaded, Prime Infrastructure displays a report of what was and was not added to Prime Infrastructure.

If some of the data to be imported already exists, Prime Infrastructure either uses the existing data in the case of campuses, or overwrites the existing data in the cases of buildings and floors.

If there are duplicate names between a WLSE site and building combination and a Prime Infrastructure campus (or top-level building) and building combination, Prime Infrastructure displays a message in the Pre Execute Import Report indicating that it will delete the existing building.

Because a WLSE file has no floor number information, the floors are imported in descending order when imported into Prime Infrastructure.

Step 6  Choose Maps > Site Maps to verify the imported data.

Troubleshooting Voice RF Coverage Issues

- Floors with either calibration or no calibration data are treated as follows:
  - Set the AP Transmit field to Max (the maximum downlink power settings). If the map still shows some yellow or red regions, more access points are required to cover the floor.
  - If the calibrated model shows red or yellow regions (where voice is expected to be deployed) with the AP Transmit field set to Current, increasing the power level of the access points might help.
Ensuring Network Services

This part contains the following sections:

- Securing Network Services
- Configuring and Monitoring IWAN
- Using Converged Access Workflow
- Configuring Application Visibility and Control
- Ensuring Consistent Application Experiences
- Troubleshooting Applications
- Monitoring Microsoft Lync Traffic
- Using Mediatrace
- Cisco Mobility Services Engine and Services
- Configuring the Cisco AppNav Solution
- Configuring the Cisco WAAS Container
- Working with Wireless Mobility
Cisco TrustSec technology uses software-defined segmentation to simplify the provisioning of security policies, to accelerate security operations, and to consistently enforce policy anywhere in the network. TrustSec is embedded technology in Cisco switches, routers, wireless, and security devices. It is a secure network architecture that extends security across the network from campus to branch to data center. TrustSec is the foundation for using the Network as an Enforcer and mitigates risk by reducing attack surface through better segmentation, whilst also increasing operational efficiency and making compliance goals easier to achieve.

In Prime Infrastructure, the TrustSec network service design enables you to choose preferred options for provisioning configurations to TrustSec-capable devices to enable 802.1X and other TrustSec functionality. You can configure wired 802_1x devices by creating TrustSec model-based configuration templates and choosing any one of the following navigation paths:

- **Services > TrustSec**
- **Configuration > Templates > Features & Technologies > Security > TrustSec > Wired 802_1x**

**Note**
For the TrustSec 5.3 platform support list, see the [Cisco TrustSec Release 5.3 System Bulletin](https://www.cisco.com/c/en/us/products/collateral/security/trustsec/white_paper_c11-687230.html).


**Generating a TrustSec Readiness Assessment Report**
TrustSec Readiness Assessment displays TrustSec-based device details such as TrustSec Feature classification.

The devices are categorized as:

- **Classification** is the process of assigning a security group tags based on identity or context (dynamically with 802.1x or MAB or web auth or statically mapped to IP, subnet, VLAN or interface). These security group tags are transmitted to the devices using inline tagging or security group tag exchange protocol (SXP).
- **Enforcement** is the process of enforcing traffic policy based on the security group tags via a secure group ACL (SGACL on switches and routers) or security group firewall (SGFW).
- **TrustSec Incapable** are devices with no classification, propagation or enforcement capabilities

To generate a TrustSec Readiness Assessment report, follow these steps:

**Step 1** Choose **Services > TrustSec > Readiness Assessment**.

**Step 2** Click **TrustSec Readiness** tab.
The TrustSec Table appears with the following types of devices:

- Classification Devices
- Enforcement Devices
- TrustSec Incapable Devices

**Step 3** Click the various device categories to view the details of the selected TrustSec-based device type. Each category displays the number of devices in percentage in a color coded circle. The color codes for each category are:

**Classification, Enforcement and TrustSec Incapable Devices:**

- Red—Number of TrustSec incapable devices.
- Light Green—Number of classification capable devices.
- Dark Green—Number of enforcement capable devices.

**Step 4** Choose the appropriate filter from the Show drop-down list to filter the devices in each category.

**Step 5** Click the Export icon to download the device details as CSV or PDF file.
Cisco Intelligent WAN (IWAN) is a system that enhances collaboration and cloud application performance while reducing the operating cost of the WAN. This system leverages low-cost, high-bandwidth Internet services to increase bandwidth capacity without compromising the performance, availability, or security of cloud-based applications. Organizations can use IWAN to leverage the Internet as WAN transport, as well as for direct access to Public Cloud applications.

Prime Infrastructure positions the IWAN wizard workflow mostly for green field customers where the IWAN services need to be enabled for the first time. The enabled IWAN service cannot be modified for brown field customers. But customers can always overwrite the last-configured service by rewriting any of these services on required sites.

You can use Prime Infrastructure to design, configure, and monitor the IWAN services for an enterprise. Cisco IWAN requires the configuration of DMVPN, PFR, AVC and QOS as part of enabling IWAN services on different devices.

**Related Topics**

- Cisco Intelligent WAN (IWAN) Design Guide
- Prerequisites for Enabling IWAN Services
- Using the IWAN Wizard

**Prerequisites for Enabling IWAN Services**

When designing or deploying IWAN services, configurations need to be decided. A network administrator needs to plan the branches on which the IWAN has to be enabled or reconfigured. In Prime Infrastructure, you can access a set of CVD validated out of the box IWAN templates by navigating to Configuration > Templates > Features & Technologies > Feature Templates. All the templates under this feature technology are tagged “IWAN”, and any new template that a user creates will automatically carry this tag and will appear in the IWAN workflow.

The tags that are automatically used for the templates are as follows:

- DMVPN: IWAN-DMVPN
- PFR: IWAN-PFR
- QOS: IWAN-QOS
- AVC: IWAN-AVC
- ZBFW: DIA-ZBFW
Prerequisites for Enabling IWAN Services

- CWS: DIA-CWS

**Note**

The Minimum software version required for the templates are as follows:

- IWAN-DMVPN–Cisco IOS Release 15.4 or later
- IWAN-PFR–Cisco IOS Release 15.4 or later
- IWAN-QOS–Cisco IOS Release 15.4 or later
- DIA-ZBFW–Cisco IOS Release 15.4 or later
- IWAN-AVC– See Configuring Application Visibility
- DIA-CWS
  - Cisco Validated Designs (CVD)-Cloud Web Security (CWS) Integrated Services Router-G2 platform from Cisco IOS Release 15.2(1)T1 or later
  - CVD-CWS-Integrated Services Router-4000 platform from Cisco IOS Release 15.5(3)S1 or later

The tags that are used for the IWAN Hub and IWAN Branch Categories based on the Device roles are as follows:

- **Hub Category:**
  - Master Controller: IWAN-HUB-Master-Controller
  - MPLS Hub: IWAN-HUB-MPLS
  - Internet Hub: IWAN-HUB-Internet
- **Branch Category**
  - Single Router Branch: IWAN-Branch-Single-Router
  - Dual Router Branch-MPLS: IWAN-Branch-Dual-MPLS
  - Dual Router Branch-Internet: IWAN-Branch-Dual-Internet

Users can create their own templates from the bundle templates or modify the out of the box design templates, which can be recreated from the CVD templates and displayed in the IWAN workflow.

Therefore, enabling the complete IWAN services through Prime Infrastructure is done based on two categories, SITE and ROLE. SITE can be HUB or SPOKE, and ROLE can be X, Y, Z, and so on. Depending on this selection, the templates will be organized and displayed in sequence for users to fill in the values. At the end of the workflow, the summary of the configurations to be deployed on the network is displayed. When the **Deploy** button is clicked, the configurations are pushed to the network.

**Important Notes**

- Ensure that the interface loopback 0 IP address is configured on all Master Controllers before deployment.
- The loopback IP of the Master Controller should be permitted in the DC-LOCAL-ROUTES prefix-list in HUB-Border-MPLS and HUB-Border-Internet routers for Border routers to reach MC.

Example:

```bash
ip prefix-list DC-LOCAL-ROUTES seq 40 permit <MC loopback0 ip>/32
```
• The DC_Prefix1 field in CVD-DMVPN-MPLS and CVD-DMVPN-Internet templates should match the DC subnet. If there is more than one subnet in DC, then the suffix “/32” can be used to include all the subnets.

Example:
- Subnet A—172.29.10.0/30
- Subnet B—172.29.10.4/30
- Subnet C—172.29.10.8/30
- DC_Prefix1(x.x.x/x)—172.29.10.0/24 /32

• In CVD-DMVPN, CVD-DMVPN-Dual-Internet, and CVD-DMVPN-Dual-MPLS templates, the subnet mask of the Loopback interface needs to be entered in the Loopback-Subnet field.
• %IPSEC-3-REPLAY_ERROR: IPSec SA receives an anti-replay error.

If this error message is seen on the HUB-Border-MPLS router, you may be able to resolve this by increasing the window size.

Example:
crypto ipsec security-association replay window-size 1024

Related Topics
• Cisco Intelligent WAN (IWAN) Design Guide
• Using the IWAN Wizard

Using the IWAN Wizard

Prime Infrastructure provides a wizard to help you design and deploy IWAN services.

Step 1 Select Services > Network Services > IWAN Enablement.
Step 2 Click Next to choose the configuration.
Step 3 Choose the category, device role, overlay protocol and the technologies (DMVPN, PFR, QoS, AVC, DIA-ZBFW, CWS) that will be enabled through this workflow.

The CWS technologies will be enabled only for Single Router Branch and Dual Router Branch-Internet.

Step 4 (Optional) Choose the Post-IWAN template that can be used for pushing the required configuration after IWAN deployment.
Step 5 Click Next to choose the devices on which you want to configure the specified features. To configure IWAN on multiple branches at the same time, select multiple devices and enter the values for each variable.
Step 6 Click Next to choose the input option.
Step 7 Click Work Flow option, the wizard will guide you through entering the necessary values for the selected configuration.
Step 8 Alternately, click Export/Import CSV option, to update all the template properties for the selected devices using CSV export/import mechanism.
   a. Uncheck the Do you want Optional Parameters check box, if you want to skip the optional fields while filling the configuration value in the CSV file.
   b. Click Export CSV to download the CSV template to your local system.
c. Enter the configuration values in the downloaded CSV template.

d. Click Import CSV to upload the updated CSV file.

**Step 9**
After entering the necessary configuration values, click Next or click CLI Summary to confirm the device and template configuration values.

**Step 10**
Schedule the deployment job using Prepare and Schedule tab, if required.

**Step 11**
Click Next or click Confirmation tab to deploy the template.

Post deployment, ensure that you enable routing between Master Controllers and Hub Border Routers and include the subnet of the loopback 0 interface as part of the routing domain.

---

**Related Topics**
- Using PKI with IWAN-DMVPN Service
- Cisco Intelligent WAN (IWAN) Design Guide
- Prerequisites for Enabling IWAN Services

---

**Using PKI with IWAN-DMVPN Service**

To use PKI certificates (for DMVPN only) in the IWAN workflow, you must first add a valid APIC-EM controller to Prime Infrastructure. See Integrating APIC-EM with Prime Infrastructure. The PKI option cannot be enabled if the CNS gateway is selected in the Global PnP/ZTD Settings (Administration > Servers > APIC-EM Controller >Global PnP/ZTD Settings). This is optional when you want to use a pre-shared key for IWAN DMVPN.

In the IWAN workflow, when the PKI option is enabled, in the back-end, the device is added to the APIC-EM Inventory and the PKI service is triggered to install the PKI certification on the device. The device can download the certificate in HTTP.

When the device is in the managed state, it can be used for IWAN provisioning. Here, PKI certificate-based authentication is done instead of using a pre-shared key.

---

**Step 1**
Choose Services > Network Services > IWAN Enablement.

**Step 2**
In the Before You Begin section, click Next.

**Step 3**
In the Choose Configuration section, select a category, device role from the drop-down lists. DMVPN, PFR, QOS, AVC values are auto-populated once the device role is selected. But these values can be edited. DMVPN is for PKI certificates only.

**Step 4**
Check the Deploy PKI check box so that the user can enable PKI certificate-based authentication for DMVPN Tunnels. Click Next.

**Step 5**
In the Select Devices section, select the devices and click Next.

**Step 6**
In the Demo_DMVPN_TEMP section, enter the values in the fields under Loopback, MPLS Tunnel and EDGRP. Click Apply and then click Next.

**Step 7**
In the CLI Summary section, the CLI commands in the DMVPN template are displayed along with the values that were entered by the user in the Demo_DMVPN_TEMP section. Click Next.

**Step 8**
In the Prepare and Schedule section, click Next if you want the job to start now and not recur. If you want the IWAN job to run at a later time in a recurring pattern, then specify the time and recurrence under Schedule. Specify the Job Option, if required.
Step 9  In the **Confirmation** section, click **Deploy** to configure the device.

Step 10  The confirmation message appears. Click **OK**. The **User Jobs** pane under **Administration / Jobs** appears. The status of the IWAN DMVPN configuration and PKI certificate provisioning on the device can be tracked in the Job dashboard.

When either of the IWAN DMVPN config or PKI fail, the overall status of the IWAN provisioning will be displayed as “Failed” and the details will display whether the IWAN DMVPN configuration or the PKI failed.

For example, if there is any failure in the PKI IWAN service, an error message “Failed to install PKI certificate on device” will be displayed on the Job page of IWAN. When PKI service fails, all jobs will fail.

**Related Topics**
- [Cisco Intelligent WAN (IWAN) Design Guide](#)
- [Using the IWAN Wizard](#)
- [Integrating APIC-EM with Prime Infrastructure](#)
Using Converged Access Workflow

Converged Access Workflow Overview

The Converged Access workflow simplifies, automates and optimizes deployment of various enterprise-class next generation wireless deployment models for campus and branch networks. Cisco Prime Infrastructure can automate the converged access deployment of wireless networks using converged access components such as Catalyst 3650, 3850, 4500 SUP 8-E switches, and Cisco 5760 Wireless LAN controller (WLC). The catalyst switches can be deployed as Mobility Agent (MA), Mobility Controller (MC), and Guest Anchor controller (GA).

Figure 46-1 illustrates the wireless converged access deployment models.
**Converged Access Workflow Overview**

**Single-Switch Small Network Deployment Model**
This deployment model assumes single Catalyst 3650, 3850 or 4500 SUP 8-E switch deployed in Access layer in combined MA and MC roles. The Catalyst switches can be deployed in individual standalone system mode or in stackwise redundant supervisor mode.

**Controller-Less Single/Multi-Domain Deployment Model**
This deployment model consists of multiple sub-domains and allows inter-domain MC peering for end-to-end seamless roaming across sub-domains. The MA switches are deployed in Access layer while the MC switches can be placed in Distribution layer.

**Controller-Based Single/Multi-Domain Deployment Model**
A large scale converged access campus building is deployed with external 5760 WLC as MC. The Access layer switches are deployed as MA across multiple buildings with centralized 5760 MC. In such large network, multiple 5760 WLCs may co-exist for better load balancing and redundancy. Depending on the roaming requirement across different buildings, the inter-domain mobility peering between 5760 WLCs can be established.

**Centralized Wireless Campus Deployment Model**
In this deployment model, the switches in Access layer remain in traditional switching mode and wireless communication between Access Point (AP) and WLC is built as overlay network. In large scale campus deployments, multiple 5760 WLCs can be deployed for better load balancing and redundancy. To provide seamless large mobility domains, the inter-domain mobility peering 5760 WLCs can be established.

**Key Benefits**
- Simple Automated Deployment—Simplifies the converged access deployment by automating the device configuration process. Requires only a few deployment specific inputs from the network administrator and pushes the complete converged access configurations to the network devices.
- Error Free Deployment—The template-based configuration used by Cisco Prime Infrastructure avoids manual misconfigurations, making it easier to build/maintain enterprise-wide standardized configurations that are well understood by the network administrator.
- Optimized Deployment—The configuration templates used by Cisco Prime Infrastructure incorporates a large number of Cisco best practice guidelines, improving the deployment quality. Some of the best practice wireless technologies/features that are automatically included in the template are Band-Select, Radio Resource Management (RRM), Fast SSID-Change, CleanAir, and Wireless QoS.
- High Scalability—Supports large enterprises with thousands of branches. It not only reduces efforts to deploy greenfield branches, but also simplifies large scale conversion of traditional Ethernet based branch networks to converged access branches in an error-free way.

**Related Topics**
- Supported Cisco IOS-XE Platforms
- Prerequisites for Converged Access Deployment
- Converged Access Template-Based Deployment
- Guidelines for Entering Configuration Values
**Supported Cisco IOS-XE Platforms**

The following tables describe the supported Cisco IOS-XE platforms for small, large, and centralized network deployment models.

### Table 46-1  Supported Cisco IOS-XE for Small Network Deployment Mode

<table>
<thead>
<tr>
<th>Device Role</th>
<th>Cisco IOS-XE Platform</th>
<th>System Mode</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Agent/Mobility Controller (Single-Switch)</td>
<td>Catalyst 3650</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
<tr>
<td></td>
<td>Catalyst 3850</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
<tr>
<td></td>
<td>Catalyst 4500 SUP 8-E</td>
<td>Single or Dual-SUP</td>
<td>3.7.0 and later</td>
</tr>
<tr>
<td>Guest Anchor WLC</td>
<td>CT5760 WLC</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
</tbody>
</table>

### Table 46-2  Supported Cisco IOS-XE for Large Network Deployment Model

<table>
<thead>
<tr>
<th>Device Role</th>
<th>Cisco IOS-XE Platform</th>
<th>System Mode</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Agent</td>
<td>Catalyst 3650</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
<tr>
<td></td>
<td>Catalyst 3850</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
<tr>
<td></td>
<td>Catalyst 4500 SUP 8-E</td>
<td>Single or Dual-SUP</td>
<td>3.7.0 and later</td>
</tr>
<tr>
<td>Mobility Controller</td>
<td>Catalyst 3650</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
<tr>
<td></td>
<td>Catalyst 3850</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
<tr>
<td></td>
<td>Catalyst 4500 SUP 8-E</td>
<td>Single or Dual-SUP</td>
<td>3.7.0 and later</td>
</tr>
<tr>
<td></td>
<td>CT5760 WLC</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
<tr>
<td>Guest Anchor Controller</td>
<td>CT5760 WLC</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
</tbody>
</table>

### Table 46-3  Supported Cisco IOS-XE for Centralized Wireless Deployment Mode

<table>
<thead>
<tr>
<th>Device Role</th>
<th>Cisco IOS-XE Platform</th>
<th>System Mode</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Controller</td>
<td>CT5760 WLC</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
<tr>
<td>Guest Anchor WLC</td>
<td>CT5760 WLC</td>
<td>Single or StackWise</td>
<td>3.6.0 and later</td>
</tr>
</tbody>
</table>
Prerequisites for Converged Access Deployment

To successfully deploy the Converged Access solution using the Converged Access Workflow, the wired infrastructure of the network should be set for further configuration required for converged access. This section describes the prerequisite configurations for Converged Access Workflow based deployment.

You can view the prerequisites using the click here link in the Before you Begin page in the Converged Access Workflow (Services > Network Services > Converged Access).

Prerequisites for Layer 2 and Layer 3

Table 46-4 describes the Layer 2 and Layer 3 prerequisites, and sample configuration for the Converged Access Workflow. In the sample configuration, the following nomenclature is used to represent the various wireless management VLANs in the MA and MC:

- WM_VLAN - Name of the Wireless Management VLAN
- WM_VLAN_id - ID of the Wireless Management VLAN
- WLAN1_Client_VLAN_Name - VLAN name of WLAN 1
- WLAN2_Client_VLAN_Name - VLAN name of WLAN 2
- WLAN3_Client_VLAN_Name - VLAN name of WLAN 3
- WLAN1_Client_VLAN_id - VLAN ID of WLAN 1
- WLAN2_Client_VLAN_id - VLAN ID of WLAN 2
- WLAN3_Client_VLAN_id - VLAN ID of WLAN 3

Note: WLANx_Client_VLAN_id represents all the three client VLAN IDs.
### Table 46-4  Layer 2 and Layer 3 Prerequisites for Converged Access Switches for Device Roles MA and MC

<table>
<thead>
<tr>
<th>Task on Converged Access Switch</th>
<th>Sample Configuration</th>
</tr>
</thead>
</table>
| **Wireless Management VLAN**    | ! Mgmt VLAN on Access Switch  
|                                 | vlan <WM_VLAN_id>  
|                                 | name <WM_VLAN>  
|                                 | ! Apply VLAN to access ports connected to Access Points  
|                                 | interface GigabitEthernet 1/0/x  
|                                 | description Connected to Access-Points  
|                                 | switchport mode access  
|                                 | switchport access vlan <WM_VLAN_id>  
| **Create Wireless Client VLANs**| ! Create the wireless Client VLANs on Access Switch  
|                                 | vlan <WLAN1_Client_VLAN_id>  
|                                 | name <WLAN1_Client_VLAN_Name>  
|                                 | vlan <WLAN2_Client_VLAN_id>  
|                                 | name <WLAN2_Client_VLAN_Name>  
|                                 | vlan <WLAN3_Client_VLAN_id>  
|                                 | name <WLAN3_Client_VLAN_Name>  
| **DHCP Snooping /ARP Inspection**| ! Enable DHCP Snooping & ARP Inspection on all WLAN Client VLANs (Static or Dynamic)  
|                                 | ip dhcp snooping  
|                                 | ip dhcp snooping vlan name <WLANx_Client_VLAN_id>  
|                                 | no ip dhcp snooping information option  
|                                 | ip arp inspection vlan <WLANx_Client_VLAN_id>  
|                                 | ip arp inspection validate source destination allow-zeros  
|                                 | interface Port-Channel <id>  
|                                 | description L2 Trunk to Upstream Router/Switch  
|                                 | ip dhcp snooping trust  
|                                 | ip arp inspection trust  
| **Switch Trunk Ports**          | ! Configure trunk port to other connected switches/router  
|                                 | interface Port-channel1  
|                                 | description Connected to Upstream System  
|                                 | switchport trunk allowed vlan add <WM_VLAN_id>, <WLAN1_Client_VLAN_id>, <WLAN2_Client_VLAN_id>, <WLAN3_Client_VLAN_id>  
|                                 | ip arp inspection trust  
|                                 | ip dhcp snooping trust  
| **Default Gateway**             | ! Configure default-gateway  
|                                 | <ip default-gateway>  
| **Wireless Mobility Controller**| wireless mobility controller  
|                                 | write memory  
|                                 | reload  

---

Wireless Management VLAN

- Create wireless management VLAN with a network wide unique name.
- Configure access ports connected to APs under this VLAN.

Create Wireless Client VLANs

- Create wireless client VLANs in VLAN database. The VLAN names are common across campus and branches.
- Enable DHCP snooping and ARP inspection on each WLAN client VLANs in the access switch (for static or dynamic VLAN).
- Configure upstream Layer 2 trunk as trusted for ARP inspection and DHCP snooping.

DHCP Snooping /ARP Inspection

- Ensure that the other ends of the trunk ports are properly configured (not shown).
- Ensure that default gateway is configured.

Wireless Mobility Controller

- If you want Catalyst 3650, 3850, and 4500 SUP 8-E switches to be deployed as MC then configure the switches as MC, and reload them to make the configuration effective.
### Table 46-5: Prerequisites for Converged Access Deployment

<table>
<thead>
<tr>
<th>Task on Converged Access Switch</th>
<th>Sample Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AP Licenses</strong></td>
<td>! Activate AP license on branch converged access switch &lt;br&gt;license right-to-use activate ap-count &lt;count&gt; slot &lt;ID&gt; acceptEULA</td>
</tr>
<tr>
<td>• MC must have sufficient AP licenses to support all APs in its sub-domain, and activate the licenses on the APs. The activation does not require a reboot. &lt;br&gt;• The GA does not require AP license.</td>
<td><strong>Security</strong>&lt;br&gt;• Convert relevant authentication commands on the access switches to their Class-Based Policy Language (CPL) equivalents. <strong>AP Licenses</strong>&lt;br&gt;• Add wireless management VLAN to the AP interface template LAP_INTERFACE_TEMPLATE . &lt;br&gt;• Apply the updated template to each switch port connected to an AP. &lt;br&gt;• Verify that the VLANs are applied using the following command: &lt;br&gt;<code>show derived-config interface &lt;interface id&gt;</code>&lt;br&gt;template LAP_INTERFACE_TEMPLATE &lt;br&gt;switchport access vlan &lt;Wireless_Mgmt_VLAN_id&gt; &lt;br&gt;! Associate the LAP_INTERFACE_TEMPLATE to switch ports connected to APs. This puts the interface in shutdown state; so issue a “no shut” command <code>interface Gig 1/0/x</code>&lt;br&gt;source template LAP_INTERFACE_TEMPLATE &lt;br&gt;no shutdown</td>
</tr>
<tr>
<td><strong>Update AP Interface Template</strong></td>
<td><strong>Update AP Interface Template</strong></td>
</tr>
<tr>
<td>• Add wireless management VLAN to the AP interface template LAP_INTERFACE_TEMPLATE .</td>
<td><strong>Update AP Interface Template</strong></td>
</tr>
<tr>
<td>• Apply the updated template to each switch port connected to an AP.</td>
<td></td>
</tr>
<tr>
<td>• Verify that the VLANs are applied using the following command: <code>show derived-config interface &lt;interface id&gt;</code></td>
<td></td>
</tr>
<tr>
<td>This step is not necessary if <code>autoconf enable</code> command is globally configured. In this case, the switch automatically detects the device types of the connected devices, and applies appropriate interface templates.</td>
<td></td>
</tr>
</tbody>
</table>

Table 46-5 describes the Layer 2 and Layer 3 prerequisites, and sample configuration for GA. In the sample configuration, the following nomenclature is used to represent the wireless management VLAN and Guest VLAN details for GA:

- WM_VLAN - Name of the Wireless Management VLAN
- WM_VLAN_id - ID of the Wireless Management VLAN
- GUEST_VLAN_Name - VLAN name of Guest Anchor Controller
- GUEST_VLAN_id - VLAN ID of Guest Anchor Controller
### Table 46-5  Layer 2 and Layer 3 Prerequisites for Guest Anchor Controller

<table>
<thead>
<tr>
<th>Task on Guest Anchor Controller</th>
<th>Sample Configuration for Guest Access Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wireless Management VLAN</strong></td>
<td>![Mgmt VLAN on Access Switch vlan &lt;NM_VLAN_id&gt; name &lt;NM_VLAN&gt;]</td>
</tr>
<tr>
<td>• Create wireless management VLAN with a network wide unique name.</td>
<td>![Create the wireless guest VLANS on Access Switch vlan &lt;GUEST_VLAN_id&gt; name &lt;GUEST_VLAN_Name&gt;]</td>
</tr>
</tbody>
</table>

| **Create Wireless Guest VLAN**  | ![Enable DHCP Snooping & ARP Inspection on Guest VLAN](ip dhcp snooping
ip dhcp snooping vlan name <GUEST_VLAN_Name>)
no ip dhcp snooping information option
ip arp inspection vlan <GUEST_VLAN_id>
ip arp inspection validate source destination allow-zeros
interface Port-Channel <id>
description L2 Trunk to network
ip dhcp snooping trust
ip arp inspection trust) |
| • Create wireless Guest VLANs in VLAN database. The VLAN name must be common across all GAs. | ![Ensure that default gateway is configured.](ip default-gateway <ip address>) |

| **DHCP Snooping / ARP Inspection**
| • Enable DHCP snooping and ARP inspection on the Guest VLAN. | ![Convert relevant authentication commands on the access switches to their Class-Based Policy Language (CPL) equivalents.](authentication convert-to new-style) |
| • Configure Layer 2 trunk connected to the network as trusted for ARP inspection and DHCP snooping. | This command permanently converts the legacy configuration on the switch to identity-based networking services. On entering this command, a message is displayed for your permission to continue. Permit the conversion. |

| **Default Gateway**
| • Ensure that default gateway is configured. | ![Security](ip dhcp snooping trust
ip arp inspection trust) |

| **Security**
| • Convert relevant authentication commands on the access switches to their Class-Based Policy Language (CPL) equivalents. | |
Prerequisites for Server Configuration

- Cisco Prime Infrastructure
  - All network-wide catalyst switches and 5760 WLCs must be configured with SNMP.
  - The Converged Access switches must be added to the inventory of Cisco Prime Infrastructure. You need to provide SNMP and Telnet credentials to add the devices to the inventory.
  - Link Cisco Prime Infrastructure with Cisco ISE engine as external server to centrally monitor end-to-end client connectivity and policy enforcement details.
- Cisco ISE/ACS
  - All network devices including catalyst switches and Guest Anchor WLC must be configured in Cisco ISE/ACS to enable centralized policy engine function.
  - AAA configuration is not required for converged access on individual network devices as it is automatically generated by Converged Access Workflow.
- DHCP Server—Internal or external DHCP server must be preconfigured with appropriate pool settings for wireless clients.
- DNS Server—Must be preconfigured with appropriate name-lookup process to successfully connect to the network.

Related Topics
- Prerequisites for Converged Access Deployment
- Prerequisites for Layer 2 and Layer 3

Converged Access Template-Based Deployment

Cisco Prime Infrastructure uses different templates for different deployment models. You need to select the appropriate template based on your network topology as explained in Table 46-6:

<table>
<thead>
<tr>
<th>Network Topology</th>
<th>Configuration Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-switch small network</td>
<td>IOS-XE Controller - Small Network</td>
</tr>
<tr>
<td>Controller-less single/multi-domain branch</td>
<td>IOS-XE Controller - Large Network</td>
</tr>
<tr>
<td>Controller-based single/multi-domain branch</td>
<td>IOS-XE Controller - Large Network</td>
</tr>
<tr>
<td>Centralized wireless campus</td>
<td>IOS-XE Centralized Wireless Network</td>
</tr>
</tbody>
</table>
To deploy a converged access template:

**Step 1** Choose **Services > Converged Access**.

**Step 2** Click **Next** to choose the deployment model.

**Step 3** From the **Select Deployment Model** drop-down list, choose any one of the following options:
- IOS-XE Controller - Small Network
- IOS-XE Controller - Large Network
- IOS-XE Centralized Wireless Network

**Step 4** Click **Next** to choose the devices to be deployed.

**Step 5** Choose the devices and click **Next** to apply the selected network configuration.

The selected device will be listed out in the left pane, and in the right pane you can configure the templates by entering the values for the Wireless Management, WLANs, Guest WLAN, Mobility, Security, Application Visibility and Control (AVC), and Quality of Services (QoS).

**Step 6** Choose the devices individually and enter the **Wireless Management** configuration values.

**Step 7** Click **Apply** and then **Next**.

**Step 8** Enter the **WLANs** configuration values that are common to all the selected devices.

By default, the **All Selected Devices** check box is enabled. You can enter the WLAN configuration values for all the devices at the same time.

**Step 9** Click **Apply** and then **Next**.

**Step 10** (Optional) Enter the **Radio** configuration values that are common to all the selected devices. By default, the **All Selected Devices** check box is enabled.

**Step 11** Click **Apply** and then **Next**.

**Step 12** (Optional) Enter the **Guest WLAN** configuration values that are common to all the selected devices.

By default, the **All Selected Devices** check box is enabled.

**Step 13** Click **Apply**.

**Step 14** Choose the devices individually and enter the **Guest Controller** configuration values.

**Step 15** Click **Apply** and then **Next**.

**Step 16** Select the individual devices and enter the **Mobility** configuration values. The Mobility configuration fields will be available in the Converged Access Wizard only for large and centralized network deployments.

**Step 17** Click **Apply** and then **Next**.

**Step 18** (Optional) Enter the **Security** configuration values that are common to all the selected devices. By default, the **All Selected Devices** check box is enabled.

**Step 19** Click **Apply** and then **Next**.

**Step 20** (Optional) Enter the **AVC** and **QoS** configuration values that are common to all the selected devices. By default, the **All Selected Devices** check box is enabled.
Step 21  Click **Apply** and then **Next** to view the confirmation screen.
The confirmation screen allows you to view the device configuration information before deployment.

Step 22  (Optional) Enter the job name and click the **Date** radio button to schedule the deployment job.

Step 23  Click **Deploy**.

---

**Related Topics**
- Prerequisites for Converged Access Deployment
- Guidelines for Entering Configuration Values


## Guidelines for Entering Configuration Values

This section provides the field descriptions for converged access template and guidelines for entering the global and local configuration values for the following deployment models with specific examples.

- Controller-less single-switch deployment model
- Controller-less single/multi-domain deployment model
- Controller-based single/multi-domain deployment model
- Centralized wireless campus deployment model

### Related Topics
- Prerequisites for Converged Access Deployment
- Converged Access Template Field Descriptions
- Entering Configuration Values for Controller-Less Single/Multi-Domain Wireless Deployment Model
- Entering Configuration Values for Controller-Based Single/Multi-Domain Wireless Deployment Model
- Entering Configuration Values for Centralized Wireless Campus Deployment Model

## Converged Access Template Field Descriptions

This section contains the field descriptions for converged access template.

### Table 46-7 Wireless Management Field Descriptions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>VLAN ID of the selected device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Wireless management IP of the selected device.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask allocated to the selected device.</td>
</tr>
</tbody>
</table>

### Table 46-8 WLAN Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>Name of the wireless LAN.</td>
</tr>
<tr>
<td>ID</td>
<td>Wireless LAN ID. If SSID &gt; 16, you need to manually enter the AP group name.</td>
</tr>
</tbody>
</table>
Guidelines for Entering Configuration Values

Chapter 46 Using Converged Access Workflow

Table 46-8 WLAN Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Allows you to customize the login window for configuring an external web server such as ISE. The following security options are available for WLAN:</td>
</tr>
<tr>
<td></td>
<td>• WPA2-Enterprise</td>
</tr>
<tr>
<td></td>
<td>• WPA2-Personal</td>
</tr>
<tr>
<td></td>
<td>• OPEN</td>
</tr>
<tr>
<td></td>
<td>For Guest WLAN, WebAuth (external) option alone is available.</td>
</tr>
<tr>
<td>Pre-Shred Key</td>
<td>This is a mandatory field, if you have a selected WPA2-Personal. The value must be alphanumeric and at least eight characters long.</td>
</tr>
<tr>
<td>Client VLAN Name</td>
<td>Name of the client VLAN. Can be alphanumeric.</td>
</tr>
<tr>
<td>AP Group</td>
<td>AP Group name is used to assign group name for the APs associated with WLAN and Client VLAN.</td>
</tr>
<tr>
<td>DHCP Required</td>
<td>This is an optional field. Check the DHCP Required check box for WLAN. This forces the wireless clients to use DHCP to get IP addresses. Clients with static address cannot access the network.</td>
</tr>
<tr>
<td>Radio</td>
<td>Radio bands used by WLAN.</td>
</tr>
<tr>
<td>Device Classification</td>
<td>You can turn on/off the device classification on the switch, using OUI and DHCP.</td>
</tr>
<tr>
<td>Device Profiling</td>
<td>You can turn on/off the device profiling. The following two options are available for device profiling:</td>
</tr>
<tr>
<td></td>
<td>• Local profiling based on HTTP attributes</td>
</tr>
<tr>
<td></td>
<td>• Radius profiling based on HTTP attributes</td>
</tr>
<tr>
<td>Client Exclusion</td>
<td>Turns on/off the client exclusion for the WLAN. When it is turned on, the misbehaving clients are added in an exclusion list so that they cannot access the network until the timeout is over. Clients may be added in the exclusion list due to excessive authentication attempts and using IP address of another client.</td>
</tr>
<tr>
<td>Client Exclusion Timeout (sec)</td>
<td>The timeout period for excluded clients.</td>
</tr>
<tr>
<td>Session Timeout (sec)</td>
<td>The timeout period for a client session. The client is re-authenticated before this period is over.</td>
</tr>
</tbody>
</table>

Table 46-9 Wireless Radio Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF Group Name</td>
<td>Name of the RF group. Multiple MCs can be placed under a single RF group, to perform RRM in a globally optimized manner and perform network calculations on a per-radio basis.</td>
</tr>
<tr>
<td>Radio 2 GHz</td>
<td>This is an optional check box.</td>
</tr>
<tr>
<td>Radio 5 GHz</td>
<td>This check box is checked by default and it’s mandatory. You cannot uncheck this check box</td>
</tr>
</tbody>
</table>
Guidelines for Entering Configuration Values

Table 46-9  Wireless Radio Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Rates</td>
<td>These data rates are disabled. Clients cannot use these data rates to connect to access points.</td>
</tr>
<tr>
<td>Mandatory Rates</td>
<td>Clients must support these data rates in order to associate to an access point, although it may connect to the AP using one of the supported data rates.</td>
</tr>
<tr>
<td>Supported Rates</td>
<td>Clients that support this data rate may communicate with the access using the supported data rate. However, clients are not required to use this data rate in order to associate with the AP.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Country code enables you to specify a particular country of operation. Configuring a country code ensures that each radio’s broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulation.</td>
</tr>
</tbody>
</table>

Table 46-10  Guest Services Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anchor Controller IP</td>
<td>Wireless management IP of Guest Anchor device.</td>
</tr>
<tr>
<td>Anchor Group Name</td>
<td>Group name of Anchor device.</td>
</tr>
<tr>
<td>Foreign Controller</td>
<td>Wireless management IP of MC to which the Guest Anchor device is associated.</td>
</tr>
</tbody>
</table>

Refer Table 46-8 for Guest WLAN field descriptions.

Table 46-11  Security Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius Server (IPs)</td>
<td>IP address of the Remote Authentication Dial In User Service (RADIUS) server.</td>
</tr>
<tr>
<td>Key</td>
<td>Password of Radius server.</td>
</tr>
<tr>
<td>Device HTTP TACACS</td>
<td>Select this in order to enable TACACS based device authentication to access the converged access device.</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
<tr>
<td>TACACS+ Server IP(s)</td>
<td>IP address of the TACACS server.</td>
</tr>
<tr>
<td>Key</td>
<td>Password of the TACACS server.</td>
</tr>
</tbody>
</table>
Guidelines for Entering Configuration Values

Chapter 46 Using Converged Access Workflow

Table 46-12 Application Services Field Descriptions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netflow Collectors (IP:Port)</td>
<td>IP—The IP address of the Prime Infrastructure server. Port—The port on which the NetFlow monitor will receive the exported data. For Cisco Prime Infrastructure the default port is 9991. Example: 172.20.114.251:9991</td>
</tr>
<tr>
<td>WLAN-1 SSID Bandwidth(%)</td>
<td>Specify the maximum bandwidth percentage allowed for first WLAN.</td>
</tr>
<tr>
<td>WLAN-2 SSID Bandwidth(%)</td>
<td>Specify the maximum bandwidth percentage allowed for second WLAN.</td>
</tr>
<tr>
<td>WLAN-3 SSID Bandwidth(%)</td>
<td>Specify the maximum bandwidth percentage allowed for third WLAN.</td>
</tr>
<tr>
<td>Guest SSID Bandwidth(%)</td>
<td>Specify the maximum bandwidth percentage allowed for Guest WLAN.</td>
</tr>
</tbody>
</table>

Table 46-13 Wireless Mobility Field Descriptions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Mobility Controller or Mobility Agent.</td>
</tr>
<tr>
<td>Controller IP</td>
<td>Wireless Management IP of Controller device.</td>
</tr>
<tr>
<td>Switch Peer Group Name</td>
<td>Peer group name in which the Agent is added.</td>
</tr>
<tr>
<td>Mobility Agent IP(s)</td>
<td>Wireless management IP of Mobility Agent devices. If you are entering more than one IP addresses, use semicolon to separate the IP addresses.</td>
</tr>
<tr>
<td>Peer Controller IP(s)</td>
<td>Wireless Management IP of peer controller device. If you are entering more than one IP addresses, use semicolon to separate the IP addresses.</td>
</tr>
</tbody>
</table>

Related Topics

- Prerequisites for Converged Access Deployment
- Converged Access Template-Based Deployment
- Entering Configuration Values for Controller-Less Single-Switch Deployment Model
- Entering Configuration Values for Controller-Less Single/Multi-Domain Wireless Deployment Model
- Entering Configuration Values for Controller-Based Single/Multi-Domain Wireless Deployment Model
- Entering Configuration Values for Centralized Wireless Campus Deployment Model
Entering Configuration Values for Controller-Less Single-Switch Deployment Model

A small-sized remote branch office or retail store may consist of a single converged access switch (standalone or stack) to provide network connectivity to the wired and wireless users.

For such network designs, the switch integrates both MC and MA functions. These networks may need guest wireless services, as well as common security and network access policy enforcement across all deployed sites.

The network administrator can use Cisco Prime Infrastructure IOS-XE Controller Small Network template to deploy converged access. Figure 46-2 illustrates the reference network for single-switch small network that shows three branch offices. Each site can be independently deployed using the workflow. Alternatively, one deployment workflow can deploy multiple sites. Prime Infrastructure allows you to configure the devices in five WLANs. Figure 46-2 illustrates three WLAN configuration scenario in the single-switch small network topology.
## Guidelines for Entering Configuration Values

### Figure 46-2  Controller-less Single-switch Small Network Model

<table>
<thead>
<tr>
<th>SSID</th>
<th>Security</th>
<th>Client VLAN Name</th>
<th>Guest VLAN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN 1</td>
<td>ABCCorp_802.1X</td>
<td>WPA2-Enterprise</td>
<td>8021x-WiFi_VLAN</td>
</tr>
<tr>
<td>WLAN 2</td>
<td>ABCCorp_PSK</td>
<td>WPA2-Personal</td>
<td>PSK-WiFi_VLAN</td>
</tr>
<tr>
<td>WLAN 3</td>
<td>ABCCorp-OPEN</td>
<td>OPEN</td>
<td>OPEN_WiFi-VLAN</td>
</tr>
<tr>
<td>Guest WLAN</td>
<td>ABCCorp_Guest</td>
<td>WebAuth-External</td>
<td>Guest_WiFi-VLAN</td>
</tr>
</tbody>
</table>
You must enter the Wireless Management configuration values separately for each device. Table 46-14 describes the Wireless Management configuration values for MA/MC (10.100.1.109) and Guest Anchor (10.99.2.242) in the single-switch small network topology shown in Figure 46-2.

Table 46-14 Sample Wireless Management Configuration Values for MA/MC (10.100.1.109) and GA (10.99.2.242)

<table>
<thead>
<tr>
<th>Data Field</th>
<th>MA/MC</th>
<th>GA</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>155</td>
<td>33</td>
</tr>
<tr>
<td>IP</td>
<td>10.101.1.109</td>
<td>10.99.2.242</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.240</td>
<td>255.255.255.240</td>
</tr>
</tbody>
</table>

After applying the Wireless Management configuration values, you must enter at least one WLAN configuration values. up to Table 46-15 describes sample configuration of three WLANs for the single-switch small network topology shown in Figure 46-2.

Table 46-15 Sample WLAN Configuration Values for MC/MA and GA

<table>
<thead>
<tr>
<th>Data Field</th>
<th>WLAN 1</th>
<th>WLAN 2</th>
<th>WLAN 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>ABCCorp_802.1x</td>
<td>ABCCorp_PSK</td>
<td>ABCCorp_OPEN</td>
</tr>
<tr>
<td>ID</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Security</td>
<td>WPA2-Enterprise</td>
<td>WPA2-Personal</td>
<td>OPEN</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>—</td>
<td>CISCO123</td>
<td>—</td>
</tr>
<tr>
<td>Client VLAN Name</td>
<td>8021X-WiFi_VLAN</td>
<td>PSK-WiFi_VLAN</td>
<td>OPEN_WiFi_VLAN</td>
</tr>
<tr>
<td>AP Group</td>
<td>Ap-group-1</td>
<td></td>
<td>Ap-group-HR</td>
</tr>
<tr>
<td>DHCP</td>
<td>Yes (Check the DHCP check box)</td>
<td>Yes (Check the DHCP check box)</td>
<td>Yes (Check the DHCP check box)</td>
</tr>
<tr>
<td>Radio</td>
<td>All</td>
<td>802.11g</td>
<td>802.11a/g</td>
</tr>
<tr>
<td>Device Classification</td>
<td>Yes (Check the Device Classification check box)</td>
<td>Yes (Check the Device Classification check box)</td>
<td>Yes (Check the Device Classification check box)</td>
</tr>
<tr>
<td>Device Profiling</td>
<td>None</td>
<td>Local</td>
<td>Both</td>
</tr>
<tr>
<td>Client Exclusion</td>
<td>Yes (check the Client Exclusion check box)</td>
<td>Yes (check the Client Exclusion check box)</td>
<td>Yes (check the Client Exclusion check box)</td>
</tr>
<tr>
<td>Timeout (sec)</td>
<td>60</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Session Timeout (sec)</td>
<td>1800</td>
<td>2000</td>
<td>300</td>
</tr>
</tbody>
</table>

After applying the WLAN configuration values, enter the Wireless Radio configuration values for all the devices at the same time. Table 46-16 shows the Wireless Radio configuration values for MC/MA and GA in the single-switch small network topology shown in Figure 46-2.
After applying the Wireless Radio configuration values, enter the Guest Services configuration values for all the devices at the same time. Table 46-17 describes the Guest WLAN configuration values for all the devices in the single-switch small network topology shown in Figure 46-2.

### Table 46-16 Sample Wireless Radio Configuration Values for MC/MA and GA

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Sample Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF Group Name</td>
<td>CA-RF</td>
</tr>
<tr>
<td>Radio 5 GHz</td>
<td>Yes (This check box is checked by default and it’s mandatory. You cannot uncheck this check box.)</td>
</tr>
<tr>
<td>Disable Rates</td>
<td>RATE_6M;RATE_18M; RATE_54M</td>
</tr>
<tr>
<td>Mandatory Rates</td>
<td>RATE_6M;RATE_18M; RATE_54M</td>
</tr>
<tr>
<td>Supported Rates</td>
<td>RATE_6M;RATE_18M; RATE_54M</td>
</tr>
<tr>
<td>Radio 2 GHz</td>
<td>No (This is an optional check box)</td>
</tr>
<tr>
<td>Disable Rates</td>
<td>—</td>
</tr>
<tr>
<td>Mandatory Rates</td>
<td>—</td>
</tr>
<tr>
<td>Supported Rates</td>
<td>—</td>
</tr>
<tr>
<td>Country Code</td>
<td>UNITED STATES</td>
</tr>
</tbody>
</table>

### Table 46-17 Sample Guest WLAN Configuration Values for MC/MA and GA

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Sample Configuration Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>ABCCorp_Guest</td>
</tr>
<tr>
<td>ID</td>
<td>15</td>
</tr>
<tr>
<td>Security</td>
<td>WebAuth-External</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>—</td>
</tr>
<tr>
<td>Client VLAN Name</td>
<td>Guest_WiFi_VLAN</td>
</tr>
<tr>
<td>AP Group</td>
<td>AP-group-guest</td>
</tr>
<tr>
<td>DHCP</td>
<td>yes (check the DHCP check box)</td>
</tr>
<tr>
<td>Radio</td>
<td>802.11a (or 802.11a/g, 802.11b/g, 802.11g, or All)</td>
</tr>
<tr>
<td>Device Classification</td>
<td>Yes (check the Device Classification check box)</td>
</tr>
<tr>
<td>Device Profiling</td>
<td>Both</td>
</tr>
<tr>
<td>Client Exclusion</td>
<td>ON</td>
</tr>
<tr>
<td>Timeout (sec)</td>
<td>100</td>
</tr>
<tr>
<td>Session Timeout (sec)</td>
<td>5000</td>
</tr>
</tbody>
</table>

Table 46-18 describes the sample Guest Controller configuration values for MC/MA (10.100.1.109) and GA in the single-switch small network topology shown in Figure 46-2.
Chapter 46      Using Converged Access Workflow

Guidelines for Entering Configuration Values

After applying the Guest Services configuration values, enter the Security configuration values for all the devices at the same time. Table 46-19 describes the sample Security configuration values for MC/MA and GA in the single-switch small network topology shown in Figure 46-2.

Table 46-19  Sample Security Configuration Values for MC/MA and GA

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Sample Configuration Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius Server (IPs)</td>
<td>10.100.1.49</td>
</tr>
<tr>
<td>Key</td>
<td>CISCO</td>
</tr>
<tr>
<td>Device HTTP TACACS Authentication</td>
<td>Yes (check the Device HTTP TACACS Authentication check box)</td>
</tr>
<tr>
<td>TACACS+ Server IP(s)</td>
<td>10.100.1.51</td>
</tr>
<tr>
<td>Key</td>
<td>cisco</td>
</tr>
</tbody>
</table>

After applying the Security configurations values, enter the AVC and QoS configuration values for all the devices. Table 46-20 describes the sample configuration values for MC/MA and GA in the single-switch small network topology shown in Figure 46-2.

Table 46-20  Sample AVC and QoS Configuration Values for MC/MA and GA

<table>
<thead>
<tr>
<th>Data Field</th>
<th>Sample Configuration Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netflow Collectors (IP:Port)</td>
<td>10.100.1.02:9991; 10.100.1.03:2055</td>
</tr>
<tr>
<td>WLAN-1 SSID Bandwidth(%)</td>
<td>40</td>
</tr>
<tr>
<td>WLAN-2 SSID Bandwidth(%)</td>
<td>30</td>
</tr>
<tr>
<td>WLAN-3 SSID Bandwidth(%)</td>
<td>20</td>
</tr>
<tr>
<td>Guest SSID Bandwidth(%)</td>
<td>10</td>
</tr>
</tbody>
</table>

Related Topics

- Prerequisites for Converged Access Deployment
- Converged Access Template-Based Deployment
- Converged Access Template Field Descriptions
- Entering Configuration Values for Controller-Less Single/Multi-Domain Wireless Deployment Model
Guidelines for Entering Configuration Values

- Entering Configuration Values for Controller-Based Single/Multi-Domain Wireless Deployment Model
- Entering Configuration Values for Centralized Wireless Campus Deployment Model
Enter the Wireless Management, WLANs, Wireless Radio, and Guest WLAN configuration values for all the devices as described in single-switch small network deployment model. Enter the Guest Controller configuration values and Mobility configuration values for MA, MC, and GA for the topology shown in Figure 46-3.
Table 46-21  Sample Guest Controller Configuration Values for MA, MC, and GA

<table>
<thead>
<tr>
<th>Data Field</th>
<th>MA</th>
<th>MC</th>
<th>GA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anchor Controller IP</td>
<td>10.99.2.242</td>
<td>10.99.2.242</td>
<td>10.99.2.242</td>
</tr>
<tr>
<td>Anchor Group Name</td>
<td>CA-Mobility-SubDomain-3</td>
<td>CA-Mobility-SubDomain-3</td>
<td>CA-Mobility-SubDomain-3</td>
</tr>
<tr>
<td>Foreign Controller</td>
<td>10.101.4.109</td>
<td>10.101.3.109</td>
<td>10.101.3.109</td>
</tr>
</tbody>
</table>

Table 46-22 describes the Mobility configuration values for MA, MC in SPG-1, and GA shown in Figure 46-3.

Table 46-22  Sample Mobility Configuration Values for MA, MC, and GA

<table>
<thead>
<tr>
<th>Data Field</th>
<th>MA</th>
<th>MC</th>
<th>GA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Agent</td>
<td>Controller</td>
<td>Controller</td>
</tr>
<tr>
<td>Controller IP</td>
<td>10.101.3.109</td>
<td>10.101.3.109</td>
<td>—</td>
</tr>
<tr>
<td>Switch Peer Group Name</td>
<td>SPG-1</td>
<td>SPG-1</td>
<td>—</td>
</tr>
<tr>
<td>Mobility Agent IP(s)</td>
<td>—</td>
<td>10.101.1.109</td>
<td>—</td>
</tr>
<tr>
<td>Peer Controller IP(s)</td>
<td>—</td>
<td>10.101.4.109</td>
<td>—</td>
</tr>
</tbody>
</table>

Repeat the same procedure for MA and MC in SPG-2 as shown in Figure 46-3.

After applying the Mobility configuration values, enter the Security, AVC and QoS configuration values as described in single-switch small network deployment model.

Related Topics
- Prerequisites for Converged Access Deployment
- Converged Access Template Field Descriptions
- Entering Configuration Values for Controller-Less Single-Switch Deployment Model
- Entering Configuration Values for Controller-Based Single/Multi-Domain Wireless Deployment Model
- Entering Configuration Values for Centralized Wireless Campus Deployment Model
Entering Configuration Values for Controller-Based Single/Multi-Domain Wireless Deployment Model

Figure 46-4 illustrates the controller-based single/multi-domain deployment model that leverages the same IOS-XE Controller Large Network template for deploying converged access with an external 5760 WLC as the MC.

Figure 46-4  Controller-Based Large Campus Model

Enter the configuration values as explained in controller-less single/multi-domain wireless deployment model.
Guidelines for Entering Configuration Values

Related Topics

- Prerequisites for Converged Access Deployment
- Converged Access Template Field Descriptions
- Entering Configuration Values for Controller-Less Single-Switch Deployment Model
- Entering Configuration Values for Controller-Less Single/Multi-Domain Wireless Deployment Model
- Entering Configuration Values for Centralized Wireless Campus Deployment Model
Guidelines for Entering Configuration Values

Entering Configuration Values for Centralized Wireless Campus Deployment Model

Cisco Prime Infrastructure IOS-XE Centralized Wireless template supports traditional wireless deployment model using next-generation 5760-WLC. In this model, any generation Access layer switches are deployed in traditional Ethernet switch mode over which WLC and the APs build an overlay network using CAPWAP Tunneling mechanism.

Figure 46-5 illustrates 5760-WLC based Centralized Wireless deployment using IOS-XE Centralized template.

Figure 46-5 Centralized Campus Network Model

Enter the Wireless Management, WLANs, Wireless Radio, and Guest WLAN configuration values for all the devices as described in single-switch small network deployment model. Enter the Guest Controller configuration values and Mobility configuration values for 5760 WLC in SPG-1 and GA for the topology shown in Figure 46-5.
Repeat the same procedure for 5760 WLC in SPG-2 shown in Figure 46-5. After applying the Mobility configuration values, enter the Security, AVC and QoS configuration values as described in single-switch small network deployment model.

**Table 46-23 Sample Guest Controller Configuration Values for 5760 WLC and GA**

<table>
<thead>
<tr>
<th>Data Field</th>
<th>5760 WLC</th>
<th>GA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anchor Controller IP</td>
<td>10.99.2.242</td>
<td>10.99.2.242</td>
</tr>
<tr>
<td>Anchor Group Name</td>
<td>CA-Mobility-SubDomain-3</td>
<td>CA-Mobility-SubDomain-3</td>
</tr>
<tr>
<td>Foreign Controllers</td>
<td>10.100.222.1</td>
<td>10.100.221.1; 10.100.222.1</td>
</tr>
</tbody>
</table>

**Table 46-24 Sample Mobility Configuration Values for 5760 WLC and GA**

<table>
<thead>
<tr>
<th>Data Field</th>
<th>5760 WLC</th>
<th>GA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Controller IP(s)</td>
<td>10.100.222.1</td>
<td>—</td>
</tr>
</tbody>
</table>

Repeat the same procedure for 5760 WLC in SPG-2 shown in Figure 46-5. After applying the Mobility configuration values, enter the Security, AVC and QoS configuration values as described in single-switch small network deployment model.

**Related Topics**

- Prerequisites for Converged Access Deployment
- Converged Access Template Field Descriptions
- Entering Configuration Values for Controller-Less Single-Switch Deployment Model
- Entering Configuration Values for Controller-Less Single/Multi-Domain Wireless Deployment Model
- Entering Configuration Values for Controller-Based Single/Multi-Domain Wireless Deployment Model
Configuring Branch Threat Defense

Cisco Branch Threat Defense is a router security technology that strengthens protection and saves time and money without having to deploy multiple-point security products. This technology mitigates security vulnerabilities in branch offices with direct Internet connections that bypass your data center, and encrypt communication between enterprise branches, headquarters, and data centers.

You can use Prime Infrastructure to configure Branch Threat Defense starting from Regulatory Compliance use cases, and configure the technologies such as Zone-Based Firewall (ZBFW), Snort Intrusion Prevention System (IPS), Cloud Web Security (CWS) and OpenDNS.

Related Topics
- Cisco Branch Threat Defense Guide
- Supported IOS-XE Platforms
- Supported IOS-XE Versions
- Prerequisites for Enabling Branch Threat Defense
- Using the Branch Threat Defense Wizard

Supported IOS-XE Platforms

The Branch Threat Defense functionality is supported on Cisco 4000 series Integrated Services Routers (ISR).

Supported IOS-XE Versions

The Branch Threat Defense functionality is available in Cisco IOS-XE Release 15.5(3)S1 (16.3.1 when OpenDNS is configured) and later releases.

Prerequisites for Enabling Branch Threat Defense

- This feature is available only in Security Packages which require a security license. Contact Cisco Support to obtain the license.
- Ensure that the Cisco 4000 series ISR has at least 8 GB of RAM. For more information, see the section “Virtual Service Resource Profile” in the Security Configuration Guide for Branch Threat Defense in the Related Topics.

- Each router to be provisioned should already have a Snort IPS OVA present in the same location on its file-system. Use the “Copy OVA to Device” CLI template to distribute a Snort IPS OVA to each device to be provisioned before proceeding.

### Related Topics
- Using the Branch Threat Defense Wizard
- Supported IOS-XE Platforms
- Supported IOS-XE Versions
- Security Configuration Guide for Branch Threat Defense

## Using the Branch Threat Defense Wizard

**Step 1** Choose **Services > Network Services > Branch Threat Defense**.

**Step 2** Click **Next** to choose the configuration.

**Step 3** Read the description in the **Choose Configuration** page and choose the required use case from the **Select a Use Case** drop-down list.

   The configuration options vary according to the selected use case.

**Step 4** Choose the required configuration options and click **Next**.

**Step 5** Choose the devices you want to configure and click **Next**.

**Step 6** Enter the configuration values or use the import/export icon to configure the ZBFW, Snort IPS CLI, CWS and OpenDNS depending on the chosen use case.

**Step 7** Click **Apply** and click **Next** to goto **CLI Summary** tab where you can confirm the device and template configuration values.

**Step 8** Schedule the deployment job using **Prepare and Schedule** tab.

**Step 9** Click **Next** and click **Deploy** in the **Confirmation** tab to deploy the Branch Threat Defense.

**Step 10** Click **Job Status** to view the job details in the **Job Dashboard**.

### Related Topics
- Prerequisites for Enabling Branch Threat Defense
- Supported IOS-XE Platforms
- Supported IOS-XE Versions
- Cisco Branch Threat Defense Guide
Overview

The GUI-based Instant Access workflow in Cisco Prime Infrastructure simplifies the Cisco Instant Access deployment, interface template management, and the FEX ports configuration. The Instant Access workflow provides complete automation for deploying Instant Access networks using Cisco Catalyst 6500/6800 series switches, each connected with up to 160 compact switches. In addition, it also automates the provisioning of FEX ports for devices to be connected either statically or dynamically via automatic device detection. Applicable Cisco best practice configurations are automatically deployed by the workflow, further minimizing the deployment efforts. The workflow not only greatly reduces the time to deploy access networks, but also provides a centralized view of the network for management purpose.

The Instant Access workflow automates the following tasks:

- VSS conversion—The workflow allows a 6500/6800 series switch to be converted to VSS mode. VSS mode is a pre-requisite for a switch to be configured with Instant Access.
- Configuring Instant Access on a VSS converted switch. This includes converting the ports on the parent switch to FEX mode.
- Creation and application of Templates, and VLANs to automatically provision FEX ports for accepting devices that can be detected dynamically, such as Cisco IP phones, Cisco Access Points, and Apple TVs.
- Automating the creation and application of Templates and VLANs for supporting devices such as laptops that cannot be detected dynamically.
- Automatically applying Cisco Best Practice configurations.
Instant Access Topology

Figure 48-1 shows a sample Instant Access topology that can be managed and configured by Cisco Prime Infrastructure.

The sample Instant Access topology shown in Figure 48-1, includes a single catalyst 6807 chassis with 2 x SUP6T and 5 line cards. Each line card has 32 Ten Gigabit ports. Each port is connected to a FEX switch and the FEX switches are connected to different endpoints (IP Phones). The parent switch can be any supported switch as listed in Supported Parent Switches.

Pre-requisites for Using Cisco Instant Access Workflow

To successfully use the Cisco Instant Access workflow, you must ensure that the following pre-requisites are met for the network devices and Cisco Prime Infrastructure system:

- Initial Device Setup—Parent switch is reachable from Prime Infrastructure with Telnet and SNMP configured.
- Device On-boarding—Parent switch is added to Prime Infrastructure Inventory.
- IOS Software—Parent switch has the recommended software version.
- Supported Platforms—Parent switch must be VSS mode capable. See Supported Parent and Client Switches.

Supported Parent and Client Switches

The Instant Access workflow requires a single catalyst 6500-E or 6800 switch as a parent and C3560CX-12PD-S, or C3560CX-8XP-D-S compact switches as clients.
Supported Parent Switches

Table 48-1 chassis and modules that are supported as the parent switch in the Cisco Instant Access workflow.

<table>
<thead>
<tr>
<th>Chassis</th>
<th>Supervisor</th>
<th>Line Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>C6807-XL</td>
<td>C6800-SUP6T-X</td>
<td>C6800-32P10G</td>
</tr>
<tr>
<td>C6500E</td>
<td>C6800-SUP6T-XL</td>
<td>C6800-32010G-XL</td>
</tr>
<tr>
<td>C6807-XL</td>
<td>VS-SUP2T-10G</td>
<td>C6800-16P10G</td>
</tr>
<tr>
<td>C6500E</td>
<td>VS-SUP2T-10G-XL</td>
<td>C6800-16P10G-XL</td>
</tr>
<tr>
<td>C6880-X-LE</td>
<td>C6880-X-LE-SUP</td>
<td>C6880-X-LE-16P10G</td>
</tr>
<tr>
<td>C6880-X</td>
<td>C6880-X-SUP</td>
<td>C6880-16P10G</td>
</tr>
</tbody>
</table>

Note

- The Instant Access workflow does not support configuring uplink ports of Sup2T and Sup6T as Instant Access RSL ports.
- Only a single chassis VSS with single or dual Supervisors is supported.

Supported IOS Images

- SUP6T—15.3(01)SY, and above

For more information on the supported IOS images on the additional devices, see the Cisco Prime Infrastructure 3.1 Supported Devices.

Supported Client Switches

The following compact switches are supported as Instant Access Clients:

- C3560CX-12PD-S
- C3560CX-8XPD-S

Key Functions of Instant Access Workflow

The key functions of Instant Access workflow are:

- VSS Conversion
- FEX Provisioning and Pre-Provisioning
- Template/Custom Template/Workgroup Creation using Access Page
- Static Assignment of Workgroups/Templates to Ports
VSS Conversion

Instant Access configuration can only be performed on a VSS converted switch, and therefore the first step in the Instant Access Workflow is to convert a parent switch to VSS mode.

**Figure 48-2  VSS Page in Instant Access Workflow**

The VSS page allows you to create a deployment profile and add an Instant Access capable switch to the deployment profile along with any user specified description such as contact details of an Administrator. A switch added to one deployment profile cannot be added to another deployment profile. If a switch added to the deployment profile is in Standalone mode, you must convert the switch to VSS mode using the Instant Access workflow. As part of the VSS conversion, Prime Infrastructure automatically archives the configuration of the switch before and after VSS conversion and applies Cisco Best Practices configuration including QoS. You can also save the pre-VSS conversion switch configuration on the switch (bootdisk: or disk0:) and/or on a remote server using TFTP or FTP.

**Key Functions**

- Detecting VSS conversion suitability—Automatically detects if a switch is suitable for VSS conversion for Instant Access Workflow, and indicates the following issues in GUI prior to conversion:
  - Unsupported switches, chassis, and SUPs.
  - Dual SUP chassis not in SSO redundancy mode.
- Automatic saving of pre/post VSS conversion switch configurations:
  - Pre-VSS configuration is always backed up in Prime Infrastructure.
  - Pre-VSS configuration can be optionally backed up locally (bootdisk:, or disk0:), and/or remotely (TFTP/FTP)
  - Post VSS configuration is automatically backed up in Prime infrastructure.
- Automatic VSS conversion:
  - VSS conversion of a single or dual SUP switch.
  - Automatic deployment of applicable VSS Best Practice recommendations.
Key Functions of Instant Access Workflow

- Allows to specify switch location.
- Displays module status—You can proceed further in the workflow when all the module reach the required status.

• Automatic deployment of Cisco Best Practice recommendation:
  - System management best practices.
  - Layer 2 best practices—VTP, spanning tree and so on.
  - Layer 3 best practices.

FEX Provisioning and Pre-Provisioning

After a switch is converted to VSS, the FEX Management page allows you to convert the Ten Gigabit ports of supported modules on the parent switch to FEX mode. To minimize the administration efforts, the Instant Access workflow automatically assigns the FEX IDs and port channel IDs to the ports excluding already used IDs, and provides an option to override them if needed. The Instant Access workflow automatically generates QoS and Cisco Best Practices code for the provisioned ports.

Key Functions

• Automatic filtering of non-FEX capable modules/ports to simplify deployment:
  - The GUI displays only the line card modules that can support FEX conversion.
  - The GUI does not allow to configure ports already having L2/L3 configurations, or connected to an incompatible switch.
  - A port with non-FEX L2/L3 configurations can be set to factory default settings, and then converted to FEX mode.

• Automated bulk FEX conversion/removal of FEX capable ports (Ten Gigabit ports):
  - To simplify deployment efforts, the FEX ids and their Port channel IDs are automatically generated by default. However, they can be manually assigned, if desired.
  - On a Cisco 6500E or 6807 chassis with SUP6T, up to 160 Ten Gigabit Ethernet ports can be converted to FEX mode, by a single GUI deployment activity (this creates 160 x 8 = 1280 FEX ports for 8 port compact switch, or 160 x 12 = 1920 FEX ports for 12 port compact switch).
  - Administrator can pre-provision the ports even if the compact switches are not connected to the parent switch. As and when they get connected, the compact switches will be converted to FEX mode providing PnP capability.
  - Fast boot functionality can be turned on/off in bulk for compact switches.
  - You can remove FEX mode configuration from FEX converted ports, simultaneously converting the connected FEX converted compact switches to standalone mode.

• Automated application of Cisco Best Practice recommendations:
  - Recommended best practice configurations are applied to RSL ports.
  - Automatically generates and applies both ingress and egress QoS configuration to RSL ports.
  - QoS configuration can be removed and/or re-applied to RSL ports.
Key Functions of Instant Access Workflow

Figure 48-3  FEX Management Page in Instant Access Workflow

The FEX Management page shows the operation mode and status of the 10 Gigabit Ethernet ports that are associated to the slots of the parent switch. Table 48-1 shows the possible operation modes and a brief description of each mode.

Table 48-1  Operation Modes of 10 Gigabit Ethernet Ports

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>The port is configured to default factory settings, if any compatible</td>
</tr>
<tr>
<td></td>
<td>compact switch in standalone mode is not detected on the port.</td>
</tr>
<tr>
<td>Standalone</td>
<td>The port having the default configuration and a compact switch in</td>
</tr>
<tr>
<td></td>
<td>standalone mode (not converted to FEX mode), is connected to the port.</td>
</tr>
<tr>
<td>Provisioned</td>
<td>The port is configured for FEX mode. A compact switch is already</td>
</tr>
<tr>
<td></td>
<td>connected to the port and has been converted to FEX mode.</td>
</tr>
<tr>
<td>Pre-Provisioned</td>
<td>The port is configured for FEX mode before any compact switch is</td>
</tr>
<tr>
<td></td>
<td>connected to the port. Once a compact switch is connected to the port,</td>
</tr>
<tr>
<td></td>
<td>it will get converted to FEX mode, and the status of the port will</td>
</tr>
<tr>
<td></td>
<td>change to provisioned from pre-provisioned.</td>
</tr>
<tr>
<td>Non-Default</td>
<td>The port has some existing layer 2 or layer 3 configurations. Instant</td>
</tr>
<tr>
<td></td>
<td>Access workflow excludes these ports from FEX conversion by default,</td>
</tr>
<tr>
<td></td>
<td>assuming that these are valid configurations for the switch to operate in</td>
</tr>
<tr>
<td></td>
<td>the network. However, the GUI allows converting these ports to factory</td>
</tr>
<tr>
<td></td>
<td>default mode and then configuring to FEX mode.</td>
</tr>
</tbody>
</table>

The operation status of each port is represented by a colored dot in the FEX page. You can view the description by hovering the mouse over the colored dot. Table 48-2 shows the description of the operation status of the FEX ports represented as a colored dot in the FEX page.
Table 48-2  Operation Status of FEX Ports

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>The port is administratively down or FEX port is offline.</td>
</tr>
<tr>
<td>Green</td>
<td>The port is up or the FEX port is online.</td>
</tr>
<tr>
<td>Blue</td>
<td>The port is pre-provisioned.</td>
</tr>
<tr>
<td>Grey</td>
<td>The port is down (not connected).</td>
</tr>
</tbody>
</table>

Table 48-3 shows the tasks that can be performed in the FEX Action Panel.

Table 48-3  Tasks Performed in FEX Action Panels

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factory Reset</td>
<td>Configures the port to factory default settings. Click the <strong>Factory Reset</strong> radio button in the Admin tab in the FEX Action Panel to perform this task. The port must be in Default or Non-Default mode to perform this task.</td>
</tr>
</tbody>
</table>
| Pre-provisioning one/more Ten Gigabit ports| Configures the port to FEX mode while no compact switch is connected to the port. This is useful when you want to configure the parent switch before the compact switches are available.  
To pre-provision a port, it must be in one of the following modes:  
- Default and shut-down (Red).  
- Default and unconnected.  
If you want to pre-provision a port irrespective of its current configuration, you must first configure the port to Factory default settings and then apply the pre-provisioning action. |
| Provisioning one/more Ten Gigabit ports    | Configures the port to FEX mode operation while the compact switch is already connected to the port. Once the port is configured, the connected compact switch will reload itself, download the image if necessary and convert itself to FEX mode.  
To provision a port, it must be in one of the following modes:  
- Standalone mode.  
- The port must be up, in Default mode, and no CDP neighbor is detected through the port.  
**Note**  
The second condition allows recovery from a situation where a FEX provisioned port is changed to Factory default configuration. In this case, the connected compact switch will still be in FEX mode and hence will not be seen as CDP neighbor. |
| Remove FEX provision from one/more ports  | The removal operation performs the following:  
- Sets the port to factory-default mode.  
- Converts the connected compact switch to standalone mode from FEX mode.  
The port must be in FEX mode (provisioned or pre-provisioned). |
| Up                                         | Brings the port up.                                                                                                   |
Chapter 48      Instant Access Workflow

Key Functions of Instant Access Workflow

Template/Custom Template/Workgroup Creation using Access Page

The Instant Access workflow automates the administration efforts to provision the FEX ports that are created by provisioning/pre-provisioning the RSL ports. The FEX ports can be connected to various endpoint devices such as Cisco IP phones, Access Points, Telepresence devices, DMP devices, Video Surveillance Cameras, and custom devices such as Apple TV, and laptops. The automation is performed by:

- Turning on Autoconf feature, and using Interface Template functionality of IOS to automatically detect the type of device connected to an access port and dynamically configuring the port with the device appropriate template.
- Creating VLANs required for the endpoint devices. The GUI automatically generates VLAN IDs excluding:
  - VLANs already used.
  - VLAN 1, static Internal VLANs (1002-1005), dynamic Internal VLANs (e.g., 1006-1013, and 3968-4031)
- User can override any generated VLAN ID.
- Updating/creating the templates with appropriate VLANs.
- Automatically enhancing/creating the templates with Cisco Best Practices code.
- Automating the creation of QoS configurations and enabling/disabling QoS on FEX ports:
  - Ingress QoS on that classifies and marks packets
  - Egress QoS for queuing
- Ensuring that QoS is either enabled on all ports of a FEX switch or is disabled on all the ports

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down</td>
<td>Shuts the port down.</td>
</tr>
<tr>
<td>Reset</td>
<td>Shuts the port down and brings it up.</td>
</tr>
</tbody>
</table>
Figure 48-4 Access Page in Instant Access Workflow

The Access page deals with the following type of endpoint devices connected to the FEX ports:

- **Well known Cisco Endpoints**—Cisco devices such as Cisco IP phones, Cisco Access Points, Cisco Telepresence device, Cisco DMP device and Cisco Video Surveillance Camera can be automatically detected by the switch. The switch comes with built-in interface templates for these devices.

- **Custom Endpoints**—Non-Cisco devices such as Apple TV that does not have any built-in template and cannot be detected by default. You can create new templates for such devices and configure the switch to automatically detect them via MAC address or OUI and apply the template.

- **Workgroups**—Devices such as laptops are not automatically detected. The Instant Access workflow allows you to create interface templates for such devices and statically apply them to interface ranges.

You can create a separate workgroup for each department (for example, accounts department, finance department, engineering department and so on) in an organization and add an exclusive VLAN for each workgroup. The Instant Access workflow also adds Cisco Best Practice code to the templates.

The Access Page allows you to do the following:

- Add/Edit/Remove the template for Cisco devices, custom device, or workgroups.
- Turn ON or OFF the LLDP based device type detection. By default, the CDP based detection is enabled.

The templates for the Cisco devices and custom endpoint devices are automatically applied to the ports, when such a device is connected, and the templates are removed when the device is disconnected. You need not do any reconfiguration when such devices are added, removed, or moved to a different port. For the Cisco devices and custom endpoint devices to work, the configuration is complete once we create the corresponding endpoint with the template and the VLAN in the Access page. For such dynamically detectable devices, additional functionality to statically assign a template to a port as provided by the Port page is not necessary, although such static assignment is possible.
Key Functions of Instant Access Workflow

Chapter 48      Instant Access Workflow

Static Assignment of Workgroups/Templates to Ports

The ports page allows static assignment of workgroup/templates to individual FEX ports or a range of FEX ports. For example, you may assign the workgroup ACCT_Workgrp with Data VLAN ACCT_VLAN to a range of ports connected to the accounts department employees, and another workgroup ENGG_Workgroup with Data VLAN Engg_VLAN to ports connected to the engineering department employees. The ports are automatically configured with the VLANs that are associated with the department. The Port page also allows you to edit the Data and Voice VLANs for the ports.

If an employee connects an automatically detectable Cisco device or custom endpoint to the port, the corresponding template is dynamically applied to the port in addition to any statically applied template. For example, if an employee attaches an IP phone to a compact switch port, and further attaches a laptop to the IP phone, two templates are applied to the same port. First, the workgroup template corresponding to the laptop must be applied statically to the port, and then the IP Phone template is automatically applied to the port on detection of the device.

Generally, in the Ports page, you need not apply templates to FEX ports to which the automatically detectable devices such as, IP Phones or Cisco Access points are connected. However, if you know that a Cisco Access Point or an Apple TV is always connected to a fixed port, you may statically apply a Cisco Access Point template or an Apple TV (custom) template to the fixed port.

The following operations can be performed on the Ports page:

- Add or remove a template to one or more selected FEX ports. When the type field is Auto it removes the existing template from the port.
- Turn on/off Auto Conf on the selected FEX ports.
- Add or remove QoS from the FEX ports—IOS allows QoS to be applied to all FEX ports of a client switch or remove QoS from all these ports (it is not possible to add QoS to some selected FEX ports of a client switch).
Using Instant Access Workflow

To create to an Instant Access deployment profile, do the following:

**Step 1** Choose **Services > Network Services > Instant Access**.

**Step 2** Click **New Deployment** to create a new deployment profile.

**Step 3** Ensure that the pre-requisites mentioned in the **Before you Begin** page are satisfied and then click **Begin**.

**Step 4** Enter the **Deployment Name** (typically a name to identify a parent switch), **Description** and click **Save**.

**Step 5** Click the **Plus** icon and choose the VSS compatible device you want to configure as instant access parent switch (6500-E or 6800 series switch).

**Step 6** Click **OK** to view the device details in the **Action Panel**.

The action panel displays relevant details of the switch including whether it is converted to VSS or not.

**Step 7** If the device is already converted to VSS mode, go to **Step 12**.

**Step 8** If the device is not configured in VSS mode, enter the Domain ID and other required details and click **Convert** to configure the device to VSS mode.

**Step 9** Click the **Activity Log** to view the VSS conversion job status.

After the VSS conversion is over, the **VSS Action Panel** displays the status of the modules as **Other** or **OK**. The modules may take more time to reach **OK** status even after the VSS conversion is completed. You must wait until the relevant modules reach **OK** status before moving to the FEX page.

**Step 10** (Optional) Enter the Location in the Action Panel and click **Set Location**.

**Step 11** Click the Save Profile icon at the top of the VSS Page to save the profile and the running configuration of the switch in its start-up configuration. We recommend you to save the running configuration periodically while configuring a switch.

**Step 12** After the VSS Action Panel displays the status of the relevant modules as **OK**, click **Next** to move to the **FEX Management** page which displays a list of the modules. If any of the modules is disabled, wait until it becomes selectable and perform the following tasks, as required:

**Pre-provisioning the Ports**

a. Click the expand icon corresponding the required parent switch module to view the available ports.

b. Choose the ports you want to pre-provision.

c. Choose the **Pre-Provisioning** operation under **Manage ports** tab in the **Action Panel**.

d. Choose the type of compact switch that you want to connect to the ports.

e. Set **Automatic IDs** and **Automatic QoS** to ON/OFF as required.

f. If Automatic ID is set to **OFF**, click the port row in the **FEX Management** window and enter unique port channel IDs and FEX IDs for the ports and click **Save**.

g. Click **Apply**.

h. Click **Deploy** to convert the selected ports to FEX mode.

**Provisioning the Ports**

a. Choose the ports that are connected to the compact switches.

b. Choose the **Provisioning** operation under **Manage Ports** tab in the **Action Panel**.

c. Set **Automatic IDs** and **Automatic QoS** to ON/OFF as required.
d. If Automatic ID is set to OFF, click the port row in the FEX Management window and enter unique port channel IDs and FEX IDs for the ports and click Save.

e. Click Apply.

f. Click the Admin tab and choose the required Admin Port and Fast Boot settings.

g. Click Deploy to convert the selected ports to FEX mode.

**Step 13** Click Next and do the following in the Interface Template page:

a. Choose the template type from the drop-down list containing workgroups, custom templates, and built-in templates.

b. Enter the Name. The Template Name gets auto-populated based on the entered Name.

c. If you choose custom template, enter the device classification type and the classification value.

d. Choose a VLAN from the available VLANs or enter the VLAN Name.

e. The VLAN ID gets auto-populated based on the chosen VLAN. When creating a new VLAN, you can override the auto-populated value of the VLAN ID.

f. Click Apply.

g. Click Deploy.

**Step 14** Click Next and do the following in the FEX Ports page.

a. Choose the FEX ports on which you want to apply the templates.

b. Choose the template type, template name, Data VLAN, and Voice VLAN in the Manage Ports tab under Action Panel.

c. Click Apply.

d. Click Deploy.

**Step 15** Click Next to view the configuration summary of the created deployment profile.

**Related Topics**

- Pre-requisites for Using Cisco Instant Access Workflow
- Supported Parent and Client Switches
- Key Functions of Instant Access Workflow
Access Network Workflow

Overview

The Access Network workflow in Cisco Prime Infrastructure automates the access switch deployment in routed access networks in enterprise branch or campus networks. This includes building and managing access VLAN database, interface template management, and access ports configuration. The Access Network workflow provides complete automation for deploying access networks using Cisco catalyst 4500, 3850, 3650, 2960XR and 2960X series switches. In addition, it also automates the static or dynamic provisioning of access ports based on automatic device detection. The workflow reduces the deployment efforts and time by automatically deploying the applicable Cisco best practice configurations and provides a centralized view of the network for management purpose.

The Access Network workflow automates the following tasks:

- Simultaneous multiple access switch configuration—Allows the administrator to provision multiple access switches simultaneously, thus reducing the network provisioning efforts. Allows automatic access switch detection from a seed device, thus minimizing the efforts to detect all the access switches connected to a distribution switch.

- VLAN Management—Allows Cisco Prime Infrastructure to create and maintain a database of access and voice VLANs used in the access layer. This database is used to configure access switches, ensuring uniformity in VLAN names and avoiding VLAN nomenclature/id mismatch errors.

- Provisioning Access Ports—Creates and applies templates and VLANS to automatically provision access ports for:
  - accepting Cisco devices that can be detected dynamically, such as Cisco IP phones, Cisco access points, Cisco video surveillance camera, Cisco TelePresence, and Cisco digital media player.
  - detecting non-Cisco devices that can be detected dynamically based on OUI or MAC address.
  - supporting devices such as laptops that cannot be detected dynamically.

- Deploys applicable Cisco Best Practice configurations, automatically.

Pre-requisites for Using Cisco Access Network Workflow

To successfully use the Cisco Access Network workflow, you must ensure that the following pre-requisites are met for the network devices and Cisco Prime Infrastructure system:

- Routed Access network—Ensure that the access switches are connected to the distribution layer via layer 3 interfaces and *ip routing* command is applied to the switches before adding them to a profile.
- Initial Device Setup—Devices are reachable from Prime Infrastructure with SSH/Telnet and SNMP configured.
- Device On-boarding—Devices are added to Prime Infrastructure Inventory.
- IOS Software—Devices have the recommended software version, see Supported Devices.
- Supported Platforms—Devices must belong the supported product families, see Supported Devices.

**Supported Devices**

Table 49-1 shows the supported switches for Access Network workflow.

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU Type</th>
<th>Mode</th>
<th>Modules</th>
<th>Minimum Software Version</th>
<th>Minimum Software License</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-C2960X</td>
<td>Copper / POE</td>
<td>Standalone</td>
<td>-</td>
<td>IOS 15.2.2E</td>
<td>LANbase</td>
</tr>
<tr>
<td>WS-C2960X</td>
<td>Copper / POE</td>
<td>FlexStack</td>
<td>-</td>
<td>IOS 15.2.2E</td>
<td>LANbase</td>
</tr>
<tr>
<td>WS-C2960XR</td>
<td>Copper / POE</td>
<td>Standalone</td>
<td>-</td>
<td>IOS 15.2.2E</td>
<td>IP Lite</td>
</tr>
<tr>
<td>WS-C2960XR</td>
<td>Copper / POE</td>
<td>FlexStack</td>
<td>-</td>
<td>IOS 15.2.2E</td>
<td>IP Lite</td>
</tr>
<tr>
<td>WS-C3650</td>
<td>Copper / POE</td>
<td>Standalone</td>
<td>-</td>
<td>IOS-XE 3.7.3</td>
<td>IPBase</td>
</tr>
<tr>
<td>WS-C3650</td>
<td>Copper / POE</td>
<td>StackWise</td>
<td>-</td>
<td>IOS-XE 3.7.3</td>
<td>IPBase</td>
</tr>
<tr>
<td>WS-C3850</td>
<td>Copper / POE / mGig</td>
<td>Standalone</td>
<td>-</td>
<td>IOS-XE 3.7.3</td>
<td>IPBase</td>
</tr>
<tr>
<td>WS-C3850</td>
<td>Copper / POE / mGig</td>
<td>StackWise</td>
<td>-</td>
<td>IOS-XE 3.7.3</td>
<td>IPBase</td>
</tr>
<tr>
<td>WS-C45xx-E</td>
<td>Copper / POE / mGig</td>
<td>Standalone</td>
<td>Single and Dual Sup (SUP7E or SUP8E), with 47xx and 46xx series line cards</td>
<td>IOS-XE 3.6.4 and above</td>
<td>IPServices</td>
</tr>
<tr>
<td>WS-C45xx-R+E</td>
<td>Copper / POE / mGig</td>
<td>Standalone</td>
<td>Single and Dual Sup (SUP7E or SUP8E), with 47xx and 46xx series line cards</td>
<td>IOS-XE 3.6.4 and above</td>
<td>IPServices</td>
</tr>
</tbody>
</table>
Using Access Network Workflow

To create an Access Network deployment profile, do the following:

**Step 1** Choose Services > Network Services > Access Network.

**Step 2** Click New Deployment to create a new deployment profile.

**Step 3** Ensure that the pre-requisites mentioned in the Before you Begin page are satisfied and then click Begin.

**Step 4** Enter the Deployment Name, Description and click Save.

**Step 5** Click Add Devices in the Action Panel and choose the devices you want to configure.

**Step 6** Click Add.

The Cisco Best Practice configuration will be automatically added to the new devices.

**Step 7** Alternately, you can add the devices by entering the seed device IP address to display the list of CDP neighbors of the seed device.

**Step 8** Click Yes in the popup window, if you want to take back up of the device running configuration to the device local storage.

The Activity Log shows the Best Practice configuration job status and the back up job status of the newly added devices. You must wait until the jobs reach Completed status before moving to the Access Management page. If there are some errors in the Activity Log, the device may have some incompatible configurations that cause CLI deployment errors. Go to Administration > Dashboards > Job Dashboard to see more information about the CLI errors. You can remove the failed devices, correct the errors, and add the device again.

**Step 9** (Optional) If you want to remove any device from the Device Group pane, choose the device and click Remove Devices in the Action Panel.

**Step 10** Click Next to move to the Access Management page to Add, Remove or Update the interface templates.

**Step 11** Click the Add radio button in the Action Panel and do the following:

- a. Choose the template type from the drop-down list containing workgroups, custom templates, and built-in templates (endpoints).
- b. Enter the Name. The Template Name gets auto-populated based on the entered Name.
- c. If you choose custom template, enter the device classification type and the classification value.
- d. Choose a VLAN from the available VLANs or enter a new VLAN Name.
  
  If the VLAN does not exist, the workflow automatically creates a VLAN ID for the entered VLAN name. The VLAN name is expected to be common across switches, but may be associated with different VLAN IDs in different switches.
- e. Click Apply.
- f. (Optional) If you want to manually enter the VLAN ID when creating a new VLAN, click the VLANs tab in the Action Panel and set the Auto VLAN ID to OFF and enter the VLAN ID in the table.
- g. Click Deploy.

**Step 12** If you see templates with a red i icon indicating that these templates are missing in some devices or out-of-sync with other devices, choose Update to redeploy these templates to all devices to keep them in sync or choose Remove to remove the unwanted templates.

**Step 13** Click Next to move to the Ports Management page to manage port groups, configure and administrate ports.
Step 14  Click the Add radio button and do the following in the Action Panel to create a new port group.
   
a. Enter the Group Name.
   
b. Choose the port group type from the drop-down list containing workgroups, custom groups, and built-in groups (endpoints).
   
c. Set the AutoConf and AutoQoS options to ON or OFF based on the chosen port group type.
   
d. Click Deploy.

Step 15  Click the Port Config tab in the Action Panel to bind the ports to port groups or configure individual ports.
   
a. Choose the device ports in the Ports Pane.
   
b. Click the Group Binding radio button in the Action Panel.
   
c. Choose the port group from the Group Name drop-down list to add the selected ports to the port group.
   
d. Click Apply.
   
e. Click Deploy.
   
f. Choose the device ports in the Ports Pane and click the Configure Ports radio button.
   
g. Choose the template type, template name, Data VLAN, AutoConf and Voice VLAN in the Action Panel.
   
h. Click Apply.
   
i. Click Deploy.
   
j. Choose the device ports in the Ports Pane and click the QoS Policy radio button and set the Automatic QoS to ON/OFF as required.

   QoS is not automatically enabled on the ports. If required, you can enable the Automatic QoS in the action panel. While enabling Automatic QoS, do not select the trunk ports, L3 ports or ports with existing QoS policies.
   
k. Click Apply.
   
l. Click Deploy.

Step 16  Click the Admin tab in the Action Panel and do the following:
   
a. Choose the ports in the Ports pane.
   
b. Click the Up, Down, or Reset radio buttons as required to change the port status.
   
c. Click Deploy.

Step 17  Click Next to view the configuration summary of the created deployment profile.

Related Topics

* Pre-requisites for Using Cisco Access Network Workflow
* Supported Devices
Configuring Application Visibility and Control

Use configuration templates in Cisco Prime Infrastructure to design the set of device configurations that you need to set up the devices in a branch or change the feature configuration for a device from the Device Work Center.

Related Topics
- Configuring the Device using WSMA
- Configuring Application Visibility
- Managing Data Sources
- Enabling Data Deduplication
- Configuring an Easy VPN Server
- Redirecting HTTP and HTTPS Traffic
- Configuring Interfaces
- Configuring Cellular WAN Interfaces
- Configuring Network Address Translation (NAT)
- Configuring DMVPN
- Configuring GETVPN
- Creating a Zone-Based Firewall
- Creating a Routing Protocol

Configuring the Device using WSMA

Prime Infrastructure mainly uses the CLI method (over Telnet or SSHv2) to configure the devices. You can use WSMA (over SSHv2) for configuring specific features on the ASR and ISR devices. Cisco Web Services Management Agent is a more efficient and more robust method to configure the devices. Prime Infrastructure supports Zone Based Firewall and Application Visibility configuration via WSMA on the ASR and ISR devices.

To configure Zone Based Firewall or Application Visibility via WSMA, follow these steps:

Step 1 Add or edit the device in Prime Infrastructure to use SSHv2 (rather than Telnet) as the management transport protocol.
   a. When you add the device with automatic discovery, enter the SSH credentials.

Text Part Number:
b. When you add the devices manually, in Step 2, select SSH2 as the protocol.

**Step 2** If the device is also managed by Prime Infrastructure which is not configured to use SSH2, edit the device credentials:

a. Choose **Inventory > Device Management > Network Devices.**

b. Select the device and click **Edit.**

c. Change the protocol to **SSH2.**

d. Click **Update.**

**Step 3** Activate a WSMA profile on the device by configuring a WSMA configuration profile as follows:

```
#configure terminal
wsma agent config profile PIwsmaConfigServiceSSH
#exit

#wsma profile listener PIwsmaConfigServiceSSH
no wsse authorization level 15
transport ssh subsys wsma-config
#exit
```

**Step 4** Configure a configuration archive, which will be used by WSMA for handling transactional configurations and rollbacks by using the following CLI commands on the device:

```
#configure terminal
archive
log config
hidekeys
path flash:roll
maximum 5
#end
```

**Related Topics**

- Cisco IOS Configuration Fundamentals Command Reference Guide
- WSMA Configuration Guide

---

**Configuring Application Visibility**

The Application Visibility feature allows you to monitor traffic on specific interfaces and generate performance and bandwidth-statistics reports that supply information to the various dashlets and reports in Prime Infrastructure. Devices send these reports to Prime Infrastructure, and each report supplies information to a subset of the Prime Infrastructure dashlets and reports. Prime Infrastructure can configure Application Visibility either through CLI (over Telnet or SSH) or through WSMA. Application Visibility can be configured through WSMA in a more efficient and robust method and we recommend that you use the WSMA protocols for configuring Application Visibility. For more information on using WSMA with Prime Infrastructure.

The Application Visibility feature is supported on the following platforms:

- ASR 1000 series platform from Cisco IOS-XE Release 15.3(1)S1 or later
- ISR G2 platform from Cisco IOS Release 15.2(4)M2 or later as listed below:
  - Cisco 1900 Series Integrated Services Routers
  - Cisco MWR 1900 Mobile Wireless Routers
- Cisco 2900 Series Integrated Services Routers
- Cisco 3900 Series Integrated Services Routers
- Cisco 812 CiFi Integrated Services Routers
- Cisco 819 Non-Hardened Integrated Services Router
- Cisco 819 Hardened Integrated Services Router
- Cisco 819 Hardened 3G - Dual Radio 802.11n WiFi ISR
- Cisco 861,861W Integrated Services Router G2
- Cisco 867,867W Integrated Services Router G2
- Cisco 866VAE Integrated Services Router
- Cisco 880 3G Integrated Services Router G2
- Cisco 881,881W Integrated Services Router G2
- Cisco 881SRST,881SRSTW Integrated Services Router G2
- Cisco 881W,881WD Integrated Services Router
- Cisco 886,886W Integrated Services Router G2
- Cisco 886SRST,886SRSTW Integrated Services Router G2
- Cisco 886VA,886VAG Integrated Services Router G2
- Cisco 886VA-W Integrated Services Router G2
- Cisco 887,887W Integrated Services Routers G2
- Cisco 887V Integrated Services Router G2
- Cisco 886VA Integrated Services Router G2
- Cisco 887VA M Integrated Services Router G2
- Cisco 887VA-W Integrated Services Router G2
- Cisco 888,888W,888GW Integrated Services Router G2
- Cisco 888ESRST,888ESRSTW Integrated Services Router G2
- Cisco 888E,888EW Integrated Services Router G2
- Cisco 888EA Integrated Services Router G2
- Cisco 888SRST,888SRSTW Integrated Services Router G2
- Cisco 891,891W Integrated Services Router G2
- Cisco 892,892W Integrated Services Router G2
- Cisco 892F,892FW Integrated Services Router
- Cisco C892FSP Integrated Services Router
- Cisco C897VA Integrated Services Router
- Cisco C897VAW Integrated Services Router
- Cisco C891F Integrated Services Routers

- ISR 4300 and 4400 series platform from Cisco IOS-XE Release 15.3(2)S or later
- CSR platform from Cisco IOS-XE Release 15.3(2)S or later
Application Visibility is configured differently on different platforms and IOS releases. Newer IOS releases provide new mechanisms with better performance for setting up the Application Visibility and Control (AVC). Thus when upgrading an ASR 1000, CSR or ISR 4400 platforms running IOS-XE release prior to 15.4(1)S to an IOS-XE release 15.4(1)S or later, or when upgrading an ISR-G2 platform running IOS release prior to 15.4(1)T to IOS release 15.4(1)T or later, we recommend that you re-configure the AVC on these devices.

To simplify configuration, the Application Visibility feature is split into four types of metric and NetFlow reports:

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Statistics</td>
<td>Sends the statistics on the bandwidth consumed by each of the NBAR-recognized applications on a per-user and per-interface basis. This report supplies information to the various application bandwidth dashlets and reports in Cisco Prime Infrastructure as “Top N Applications”, “Application Bandwidth reports”, “Top N clients”, and so on.</td>
</tr>
<tr>
<td>HTTP URL Visibility</td>
<td>Sends performance and bandwidth reports for HTTP-based traffic, and this report supplies information to various URL dashlets and reports in Cisco Prime Infrastructure as “Top N URL by hits” and “Top N URL by response time”. Note The HTTP URL Visibility tool is not supported on the ISR-G2 device.</td>
</tr>
<tr>
<td>Application Response Time</td>
<td>Sends performance-related information for TCP traffic, and this report supplies information to various response time dashlets and reports in Cisco Prime Infrastructure as “applications ART analysis”, “worst N clients by transaction time”, and so on.</td>
</tr>
<tr>
<td>Voice/Video Metrics</td>
<td>Sends various RTP key-performance indicators for RTP-based voice/video traffic, and supplies information to dashlets and reports in Cisco Prime Infrastructure under the voice/video category as “worst N RTP streams by packet lost.”</td>
</tr>
</tbody>
</table>

Activating the Application Visibility feature can impact device performance. To minimize the potential impact, the template allows you to select the traffic interfaces to monitor and the reports to generate.

To configure application visibility in your network:

1. (Optional) Set up WSMA on the devices to assure that the devices is configured via the WSMA protocol, rather than CLI. WSMA provides a more robust configuration mechanism.

2. Make sure that your devices are running an up-to-date NBAR protocol packs.

3. Estimate the potential resources impact on the device (CPU and memory) before activating application visibility on the device.

Activate application visibility on the device, either by creating a template and pushing it across the network, or by enabling AVC on an interface from the Device Work Center.

Related Topics
- Configuring the Device using WSMA
- NBAR Protocol Packs
- Activating or Deactivating a Troubleshooting Session
• Creating an Application Visibility Template
• Enabling Default Application Visibility on an Interface

Estimating CPU, Memory and NetFlow Resources on ASR Devices

The Readiness Assessment feature allows you to estimate CPU consumption, memory usage, and NetFlow export traffic when you deploy application visibility features on an ASR device. DRE helps you analyze the demands for these resources on ASR devices based on typical predefined traffic profiles and device interface speeds.

DRE is supported on all ASRs running Cisco IOS-XE Release 15.3(1)S1 or later with one or more of these modules installed:
• cevModuleASR1000ESP5
• cevModuleASR1000ESP10
• cevModuleASR1000ESP20
• cevModuleASR1001ESP
• cevModuleASR1002FESP

To estimate the resource utilization on a specific device, follow these steps:

Step 1 Choose Services > Application Visibility and Control > Readiness Assessment.
Step 2 In the Interface column for the device that you want estimates on, click the down arrow icon. The list shows only those interfaces supporting Application Visibility capability.
Step 3 Select Internet Profile or Enterprise Profile. The device resource estimation is based on a typical traffic profile. Select “Internet Profile” for typical service-provider traffic, or “Enterprise Profile” for a typical enterprise-traffic.
Step 4 Select the interfaces for which you want to estimate the resource utilization. Speeds shown are those currently configured for each interface. If you want to base the estimate on a different speed, click Speed (Mbps) and enter a different value.
Step 5 Click Get Estimates.

The Estimated Resource Usage graph displays the current, additional, and total usage of the CPU and memory, along with the threshold limit for these resources. The estimated and maximum NetFlow export traffic are also given. For devices on which AVC is already enabled, only the current and additional usage is shown.

If resource usage is crossing threshold limits, optimize the problem device by:
• Decreasing current CPU utilization
• Increasing configured memory
• Reduce configured interface speed
• Redirecting traffic to another device
NBAR Protocol Packs

The ability of the device to produce application visibility reports is based on the NBAR technology; NBAR, or Network-Based Application Recognition, is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/User Datagram Protocol (UDP) port assignments.

NBAR is updated frequently to support new applications and protocols, the software update for an NBAR is called a Protocol Pack.

Further information on NBAR protocol packs and information on how to upgrade NBAR protocol pack.

When you upgrade an NBAR protocol pack on the device, a corresponding Prime Infrastructure update should be performed to update Prime Infrastructure with the supported protocols/applications on the devices.

To achieve that there is a periodic Prime Infrastructure software update (UBF file) issues when new protocol packs are released. Once you upgrade the NBAR protocol pack on the device, you should use Prime Infrastructure software upgrade to make sure Prime is also updated with the latest protocols.

At every point of time the network may contain various platforms (ISR-G2/ASR) running different Cisco IOS software releases and different protocol pack releases. While we do not recommend that you have different protocol pack releases installed on different devices reporting application visibility reports simultaneously, Prime Infrastructure will be able to support this, by configuring only the supported subset of protocols/applications, defined as filtering conditions in your template, on each of the devices, when deploying an application visibility template across multiple devices running different versions of NBAR protocol packs.

Related Topics
- NBAR Protocol Packs Guide

Creating an Application Visibility Template

An application visibility monitoring policy is defined on a selected group of interfaces. When you define the template, ensure that you have defined an interface-role object which matches the group of interfaces on which you would like to monitor the traffic and generate NetFlow reports.

To create an Application Visibility template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Application Visibility > AVC Configuration.
Step 2 In the Template Basic area, enter a unique name and a description in the appropriate fields.
Step 3 In the Validation Criteria area, choose a device type from the list and enter the OS version.
Step 4 In the Template Detail area, choose an Interface Role from the drop-down list. The interface role designates the group of interfaces on which you can monitor the traffic and produce Application-Visibility reports.
Step 5 In the Traffic Statistics area, you can determine which traffic should be monitored to produce the traffic statistics reports, select the Off radio button if you do not want to collect the statistics on data packets.
   a. Select the IP address/subnets. You can generate the report only on IPv4 traffic. We recommend to configure the required minimal set of filter.
Step 6 In the HTTP URL Visibility area, you can select the traffic that should be monitored to produce the report. Select the Off radio button if you do not want to collect URL statistics.

a. Select the IP address/subnets. You can select a specific set of IPv4 addresses or subnets to be monitored.

b. Select the application from the drop-down list. You can select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all of the enterprise related http-based applications are include in the list.

Step 7 In the Application Response Time area, you can determine the traffic that should be monitored to produce the application response time reports. Also, optionally set a sampling option for the reports. Select the Off radio button if you do not want to collect ART metrics.

a. Select the IP address/subnets. You can select a specific set of IPv4 addresses or subnets to be monitored.

b. Choose the Application from the drop-down list. You can select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all of TCP traffic is monitored.

c. In the Advanced Options, choose the Sampling Rate from the drop-down list. In High scale environments, collecting performance indicators for every TCP conversation can lead to high resources consumption on the device. The sampling option provides the ability to further optimize the resource consumption by collecting the performance indicators for “1” out of every “n” TCP conversation. This advanced option can be used to activate sampling and select the sampling rate for the tool. It is not recommended to activate sampling as activating sampling leads to less accurate results. Sampling should be used when it is necessary to limit the resource consumption on the devices.

Note Sampling option is not applicable for ISR-G2 routers. This option will be ignored for the n ISR-G2.

Step 8 In the Voice/Video metrics area, you can determine the traffic that should be monitored to produce the voice/video reports. Select the Off radio button if you do not want to collect the voice/video metrics.

a. Choose the IP address/subnets. You can choose a specific set of IPv4 addresses or subnets to be monitored.

Note IP filtering is not supported on the ISR-G2 routers until all UDP traffic is monitored.

b. Choose the Voice/Video Application from the drop-down list. You can choose a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all RTP enterprise-related applications are monitored.

Step 9 Click Save as New Template.

Related Topics
- Creating an Interface Role
Enabling Default Application Visibility on an Interface

From the Device Work Center, you can view the reports that are generated on each of the interfaces and enable or disable a default Application Visibility configuration on selected interfaces.

When a device does not have an application visibility configuration deployed on it, or it has a default application visibility configuration deployed on it (if all metrics are collected with a set of default parameters), the Device Work Center allows you to enable or disable a default application visibility configuration on the device by selecting interfaces on the device and enabling or disabling the default configuration on the interfaces.

**Note**

When you deploy an application visibility template to the device, the application visibility template configuration will overwrite the default application visibility configuration that was enabled from the Device Work Center.

The default configuration collects all the possible visibility metrics on all applicable IPv4 traffic.

**Note**

The Application Visibility feature is supported on the following platforms:

- ASR platform from Cisco IOS-XE Release 15.3(1)S1 or later
- ISR G2 platform from Cisco IOS Release 15.2(4)M2 or later
- ISR G3 platform from Cisco IOS-XE Release 15.3(2)S later
- CSR platform from Cisco IOS-XE Release 15.3(2)S later

**Note**

Application Visibility is configured differently on the ASR platform running Cisco IOS-XE15.3(1)S1 in comparison to Cisco IOS-XE15.3(2)S or later releases. After an ASR platform Cisco IOS release is upgraded from Cisco IOS-XE15.3(1)S1 to Cisco IOS-XE Releases 15.3(2)S and later, we recommend that you reconfigure Application Visibility on those devices.

To change the default application visibility configuration profile configured on the device, first disable the Application Visibility policy on all interfaces and then re-enable it on the selected interfaces with the new profile.

To enable or disable the default application visibility configuration on the specific interface, follow these steps:

1. Choose **Inventory > Device Management > Network Devices**.
2. After choosing the device from list, click **Configuration**. The Feature Configuration pane appears.
3. Expand the **App Visibility & control** folder and choose **App Visibility**.
4. Do one of the following:
   - To activate an out-of-the-box AVC profile on an interface, select one or more interfaces then click **Enable App Visibility** and select the required profile. If at least one of the non-selected interface is attached to a different profile, a warning message will be displayed such that all non-selected interfaces that are attached to a different profile will be detached from that profile.
   - Use the interfaces list to view the current App Visibility configuration on the device. The column **App Visibility Policy** displays the current profile/policy attached to the interface.
Chapter 50  Configuring Application Visibility and Control

Configuring Application Visibility

Note The application visibility feature displays the user defined AVC policy per interface on the application visibility interfaces.

There are several options that can be displayed:

- If the application visibility control is configured on the interface using the Application Visibility Template, the template-name will be displayed.
- If the application visibility control is configured on interface using the “one-click” option, the name of the AVC Profile that was configured will be displayed.
- If the application visibility control is configured manually out-of-band by the user via CLI, the name of the policy-map or performance monitor context that was configured will be displayed.

Note A visual indication column (App Visibility Status) provides indication on whether AVC is currently activated on the interface. The column will also indicate cases when the interface is INCAPABLE of running AVC and cases when AVC is mis-configured on the interface (e.g. AVC configured to send netflows to servers other than prime infrastructure).

- To Disable any of the Activated AVC profiles on an selected interface, click Disable App Visibility, check Deactivate App Visibility Troubleshooting if you also wish to deactivate an AVC troubleshooting policy if such is active on the interface.

Note When Enabling/Disabling AVC a pop up message will appear before the actual provisioning takes place. Selecting the CLI preview tab on that popup message will generate the list of CLIs to be pushed to the device.

Application Visibility Troubleshooting Sessions

You can collect application visibility data on every flow that goes through the monitored interface. However, because this can have a significant impact on the device performance, application visibility data is collected in an aggregated manner. To further troubleshoot specific flows, you can activate the Application Visibility troubleshooting sessions on the device. The sessions are activated on specific interfaces and on specific traffic. They allow you to collect the non aggregated information on a flow-based level that supplies a raw-NetFlow report in Prime Infrastructure. This information can be used later to analyze specific flows.

The Application Visibility Troubleshooting feature allows you to:

- Create and activate a troubleshooting session on a specific interface
- Deactivate and delete a troubleshooting session on a specific interface

Caution To avoid overloading the server, we recommend that you configure no more than ten active troubleshooting sessions. Application troubleshooting is not supported on the ISR-G2 platforms.
Note

Troubleshooting sessions are configured differently on the ASR platform running Cisco IOS-XE Release 15.3(1)S1 in comparison to Cisco IOS-XE Release 15.3(2)S or later releases. After, an ASR platform Cisco IOS Release is upgraded from Cisco IOS-XE Release 15.3(1)S1 to Cisco IOS-XE Release 15.3(2)S or later, we recommend that you deactivate and reactivate active troubleshooting sessions on those devices.

To troubleshoot Application Visibility, follow these steps:

Step 1 Choose Services > Application Visibility & Control > Application Troubleshooting.

Step 2 In the AVC Troubleshooting Session page, click Add and enter a session name.

Step 3 In the Source/Destination IPs field, click Edit, and choose the source and destination IP addresses from the drop-down list. You can select the IP traffic and collect Application Visibility troubleshooting information for that specific IP traffic. The options are: on all IPv6 traffic or on all IPv4 traffic or on specific IPv4 addresses/subnets. Also, you can select a list of IP constraint pairs. Each such pair designates a bi-directional symmetric condition on the source and destination IPs of the traffic. For example, the pair: Any IPv4 <=> IPv4 subnet 192.168.0.0/16 matches all of the flows from 192.168.0.0/16 to any other IP and vice-versa (all of the flows from any IP address to 192.168.0.0/16). You can add multiple pair conditions.

Step 4 To add more IP constraints in the format of IP source/destination pairs, click the + icon in the Select Source Destination dialog box.

Note

The IP addresses on both sides of the pairs should be of the same IP version.

Step 5 Click OK.

Step 6 Choose the device from the Device Table list.

Step 7 Choose the interface from the Interface Table list.

Step 8 Choose the application from the object selector dialog box. When you choose the applications, you can have a combination of Categories, Sub-categories, Encrypted Applications, and Tunneled Applications from the available list. A maximum of 32 applications or categories or attributes can be selected.

Step 9 Click Save to automatically activate the session.

Step 10 After the troubleshooting session is activated, click Launch Report to generate the Raw NetFlow report.

Activating or Deactivating a Troubleshooting Session

You can activate an inactive troubleshooting session or deactivate an existing troubleshooting session.

To activate or deactivate a troubleshooting session, follow these steps:

Step 1 Choose Services > Application Visibility & Control > Application Troubleshooting.

Step 2 Choose a troubleshooting session from the list and click Activate or Deactivate.

Step 3 Click Save.
Editing or Deleting a Troubleshooting Session

You can edit or delete an inactive troubleshooting session. (To edit or delete an active session, you must deactivate it first.)

To edit or delete a troubleshooting session, follow these steps:

**Step 1**
Choose Services > Application Visibility & Control > Application Troubleshooting.

**Step 2**
Do either of the following:

a. Choose a session from the list and click **Edit**.

Caution
To avoid overloading the server, we recommend that you configure no more than ten active troubleshooting sessions.

b. Edit and save the troubleshooting session, then click **Activate**.

c. To delete a troubleshooting session, choose a session from the list and click **Delete**.

Managing Data Sources

Prime Infrastructure depends on a variety of sources for accurate gathering and reporting of device, performance and assurance data. These sources include specialized monitoring devices such as NAMs, and protocols running on normal devices, such as Cisco Medianet, NetFlow, Flexible NetFlow, Network Based Application Recognition (NBAR), Performance Monitoring (PerfMon), and Performance Agent.

You will want to manage these sources to ensure that only the correct data is gathered from active sources. The Data Sources page allows you to review your current data sources, and delete those that are no longer active.

For details on the data sources used in dashlets, see “Advanced Monitoring” in Related Topics. For details on setting up individual data sources, see the data-source configuration sections of “Administrator Setup Tasks”, also listed in Related Topics.

Related Topics

- Viewing Current Data Sources
- Deleting Data Sources
- Advanced Monitoring
- Administrator Setup Tasks
- Configuring Data Sources for Prime Infrastructure With Assurance
- Enabling Medianet NetFlow
- Enabling NetFlow and Flexible NetFlow
- Deploying Network Analysis Modules (NAMs)
- Enabling Performance Agent
### Viewing Current Data Sources

Use the Data Sources page to review Prime Infrastructure’s current data sources.

**Step 1**
Select **Services > Application Visibility & Control > Data Sources**. Prime Infrastructure displays a summary page that lists each data source’s:

- **Device Name**—The host name of the data source
- **Data Source**—The IP address of the data source.
- **Type**—The type of data the source is sending to Prime Infrastructure (example, “NetFlow”).
- **Exporting Device**—The IP address of the device exporting the data to Prime Infrastructure.
- **Last 5 min Flow Read Rate**—The flow rate for the data Prime Infrastructure has received from this source during the last five minutes.
- **Last Active Time**—The latest date and time that Prime Infrastructure received data from this source.

**Step 2**
For additional details on the Data Source’s configuration template or for a Device 360 view of the Exporting Device, click the “i” icon shown next to the Data Source or Exporting Device listing.

### Deleting Data Sources

Use the Data Sources page to delete inactive Prime Infrastructure data sources.

Note that you cannot delete a NetFlow data source until seven full days have elapsed without receipt of any data from that source. This delay helps protect the integrity of NetFlow data (which Prime Infrastructure identifies and aggregates according to source) by giving network operators a full week to ensure that the data source has been retired. If the source becomes active again at any time during that seven-day period, its data will still be identified and aggregated properly with other data from the same source. If the source is deleted after seven days, and then becomes active again, all of its data will be identified and aggregated as coming from a new source.

**Step 1**
Select **Services > Application Visibility & Control > Data Sources**.

**Step 2**
Select the checkbox next to the inactive data source you want to delete.

**Step 3**
Click **Delete**.

**Step 4**
Click **OK** to confirm the deletion.

### Related Topics

- Managing Data Sources
- Deleting Data Sources

- Managing Data Sources
- Viewing Current Data Sources
Enabling Data Deduplication

Data deduplication allows you to identify authoritative data sources for the corresponding location groups.

Prime infrastructure stores all the data it receives about network usages from all the sources (including any duplicate data that it may receive from multiple sources). When you specify authoritative data sources, only the data from the specified source is displayed when you view a particular site.

The data deduplication page allows you to specify a data source per a specific site. For example if you have a Network analysis module (NAM) at a branch office as well as Netflow data that is sent from the same branch, you can choose to see the site information as it is reported by the NAM or netflow data with authoritative data source.

The two authoritative data sources are

- System detected – Based on the managed device product families. You can change the device family selection precedence. To change the precedence, click on the settings icon and drag and drop the device families. The authoritative datasources are selected according to this precedence.
- Customized – You can pick and choose from the managed data source.

---

**Step 1** Choose **Services > Application Visibility & Control > Data Deduplication**. The Data Deduplication page appears

**Step 2** Click **System Detected** to identify the data sources in the location group or select the customized to select the data sources.

**Step 3** Click **Save**.

**Step 4** Click **Apply**.

---

Creating a VPN Component Template

This section describes how to create various VPN component template.

Creating an IKE Policies Template

To create an IKE policies template, follow these steps:

**Step 1** Choose **Configuration > Templates > Features & Technologies > Security > VPN Components > IKE Policies**.

**Step 2** In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

**Step 3** In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS version. For more information about the required field descriptions, see the **Cisco Prime Infrastructure 3.1 Reference Guide**.
Creating a VPN Component Template

Step 4 Click **Save as New Template**. After you save the template, apply it to your devices using the procedures in *Creating Feature-Level Configuration Templates*.

---

**Creating an IKE Settings Template**

To create an IKE settings template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Security > VPN Components > IKE Settings**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version. For more information about the required field descriptions, see the *Cisco Prime Infrastructure 3.1 Reference Guide*.

Step 4 Click **Save as New Template**. After you save the template, apply it to your devices using the procedures in *Creating Feature-Level Configuration Templates*.

---

**Creating an IPsec Profile Template**

To create an IPsec profile template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Security > VPN Components > IPSec Profile**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Template Detail area, click **Add Row** and enter the required information. A transform set represents a certain combination of security protocols and algorithms. During the IPsec negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform set describes a particular security protocol with its corresponding algorithms. For more information about the required field descriptions, see the *Cisco Prime Infrastructure 3.1 Reference Guide*.

Step 5 Click **Save as New Template**. After you save the template, apply it to your devices using the procedures in *Creating Feature-Level Configuration Templates*.

---

**Creating a Preshared Keys Template**

To create a preshared keys template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Security > VPN Components > Preshared Keys**.
Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

Step 4 In the Template Detail area, click Add Row and enter the required information.

Step 5 Click Save as New Template. After you save the template, apply it to your devices using the procedures in Creating Feature-Level Configuration Templates.

---

**Creating RSA Keys Template**

To create RSA keys template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > VPN Components > RSA Keys.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Template Detail area, click Add and enter the required information.

Step 5 Select the Exportable box to generate RSA as an exportable key, then click OK.

Step 6 Click Save as New Template. After you save the template, apply it to your devices using the procedures in Creating Feature-Level Configuration Templates.

---

**Creating a Transform Sets Template**

To create a transform sets template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > VPN Components > Transform Sets.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.

Step 4 In the Template Detail area, click Add Row and enter the required information.

>Note The ESP encryption algorithm is used to encrypt the payload, and the integrity algorithm is used to check the integrity of the payload.

Step 5 Click Save as New Template. After you save the template, apply it to your devices using the procedures in Creating Feature-Level Configuration Templates.
Configuring an Easy VPN Server

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device; for example, any of the following:

- Cisco VPN 3000 concentrator
- Cisco PIX Firewall
- Cisco IOS router that supports the Cisco Unity Client Protocol

After the Cisco Easy VPN server is configured, a VPN connection is created with minimal configuration on an Easy VPN remote, such as a Cisco 800 series or 2800 series router. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

Creating an Easy VPN Server Proxy Setting Template

The Easy VPN Server Proxy feature allows you to specify the settings for Easy VPN clients. Using this feature, you do not have to manually modify the proxy settings of the web browser when you connect to the corporate network using the Cisco IOS VPN client or manually revert the proxy settings when you disconnect from the network.

To create an Easy VPN Server Proxy template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > Easy VPN Server Proxy Setting.

Step 2 Enter the basic template information.

Step 3 From the Device Type drop-down list, choose Routers.

Step 4 In the Template detail area enter a name, and choose the settings that you want to associate with the group.

Step 5 Choose the No Proxy Server option or Automatically Detect Proxy Settings option if you want the clients in this group to automatically detect a proxy server when they use the VPN tunnel.

Step 6 Choose the Manual Configuration option to manually configure a proxy server for clients in this group. If you choose this option, you should manually configure a proxy server.

Step 7 Select the Bypass proxy server for local addresses check box to prevent the clients from using the proxy server for local (LAN) addresses.

Step 8 Click Save as New Template. After you save the template, apply it to your devices using the procedures in Creating Feature-Level Configuration Templates.
Creating an Easy VPN Remote Template

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server.

Before You Begin
Create an ACL template and publish the ACL template.

To create a Easy VPN Remote template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > Easy VPN Remote.
Step 2 Enter the basic template information.
Step 3 From the Device Type drop-down list, choose Routers.
Step 4 In the Easy VPN Remote Interface Configuration area, enter the required information. For more information about the required field descriptions, see the Cisco Prime Infrastructure 3.1 Reference Guide.
Step 5 In the Easy VPN Remote connection characteristics area, enter the required information. For more information about the required field descriptions, see the Cisco Prime Infrastructure 3.1 Reference Guide.

Note If you enable identical addressing, you must first configure Easy VPN Remote in network extension mode.
Step 6 In the Remote Authentication Mechanisms area, choose the authentication method.
Step 7 In the Remote Firewall Settings area, set the firewall settings for the Easy VPN Remote connection.
Step 8 Click Save As New Template.
Step 9 Navigate to the My Templates folder and choose the template that you just saved.
Step 10 Click the Publish icon in the top-right corner, then click OK.
Step 11 Create a composite template (Composite Templates), and add the ACL and Easy VPN Remote templates to the composite template.
Step 12 Use the arrows buttons to arrange the templates in the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the EasyVPN Remote template.
Step 13 Click Save as New Template. After you save the template, apply it to your devices using the procedures in Creating Feature-Level Configuration Templates.

Creating an Easy VPN Server Template

The Easy VPN Server feature introduces server support for the Cisco VPN software client Release 3.x and later and Cisco VPN hardware clients (such as the Cisco 800, Cisco 900, Cisco 1700, VPN 3002, and PIX 501 devices). Using IP Security (IPsec), Easy VPN Server allows a remote end user to communicate with any Cisco IOS Virtual Private Network (VPN) gateway. Also, centrally managed IPsec policies are pushed to the client device by the server and helps the end user to minimize the configuration.

Before You Begin
Configuring an Easy VPN Server

Do the following:

- Create AAA method list for the group and the user by using the CLI template
- Create an IPsec Profile template
- If you will use Crypto Map, create a Transform Set template
- (Optional) Create a CLI template for RADIUS server group creation or configure the RADIUS server while creating the AAA method list
- (Optional) Create an ACL template for the split tunnel ACL in the ISAKMP Group configuration
- Create a Browser Proxy template for ISAKMP group configuration

To create an Easy VPN Remote template, follow these steps:

**Step 1** Choose **Configuration > Templates > Features & Technologies > Security > Easy VPN Server**.

**Step 2** Enter the basic template information.

**Step 3** From the Device Type drop-down list, choose **Routers**.

**Step 4** In the Interface Configuration area, choose the configuration methods and complete the fields of the interface that is configured on the device.

**Step 5** In VPN Components Assembly area, enter the Transform Set profile name that you created in the Transform Set template (**Configuring Transform Sets**) and complete the fields in this area.

**Step 6** In the Group Authorization area, enter the Method List profile name that you created in the CLI template and complete the fields in this area.

**Step 7** In the User Authorization area, enter the same Method List profile name that you created in the CLI template, and complete the fields in this area.

**Step 8** In the ISAKMP Group configuration area, click **Add Row** to add the ISAKMP Group configuration.

**Step 9** In the ISAKMP Group configuration dialog box, enter the ACL profile name that you created in the ACL template and the Browser Proxy profile name that you created in the Browser Proxy template, and complete the fields in this area.

**Step 10** Click **Save as New Template**. After you save the template, apply it to your devices using the procedures in **Creating Feature-Level Configuration Templates**.

**Step 11** Create a composite template (**Composite Templates**) and add theAAA Method List and Radius server, IPsec Profile (**Creating an IPsec Profile Template**), ACL Browser Proxy (**Creating an Easy VPN Server Proxy Setting Template**), and Easy VPN_Remote templates in the composite template.

**Step 12** Using the arrow icons to arrange the templates in a order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, arrange the ACL template first, followed by the EasyVPN_Remote template.

**Step 13** Click **Save as New Template**. After you save the template, apply it to your devices using the procedures in **Creating Feature-Level Configuration Templates**.

Creating a GSM Profile Template

To create a GSM Profile template, follow these steps:

**Step 1** Click **Configuration > Templates > Features & Technologies > Interfaces > Cellular > GSM Profile**.
Redirecting HTTP and HTTPS Traffic

ScanSafe Software as a Service (SaaS) Web Security allows you to scan the content of HTTP and HTTPS traffic. When ScanSafe Web Security is integrated with a router, selected HTTP and HTTPS traffic is redirected to the ScanSafe cloud for content scanning and malware detection.

When Cisco Integrated Services Router (ISR) Web Security with Cisco ScanSafe is enabled and the ISR is configured to redirect web traffic to ScanSafe, the Integrated Services Router (ISR) transparently redirects HTTP and HTTPS traffic to the ScanSafe proxy servers based on the IP address and port. You can configure the ISR to relay web traffic directly to the originally requested web server without being scanned by ScanSafe.
Configuring Application Visibility and Control

Chapter 50      Configuring Application Visibility and Control

Whitelisting Traffic
You can configure the ISR so that some approved web traffic is not redirected to ScanSafe for scanning. When you bypass ScanSafe scanning, the ISR retrieves the content directly from the originally requested web server without contacting ScanSafe. When ISR receives the response from the web server, it sends the data to the client. This is called whitelisting traffic.

See the Cisco ISR Web Security with Cisco ScanSafe Solution Guide for more information about ScanSafe.

Creating a ScanSafe Template
To create a ScanSafe template, you must specify:

- The ScanSafe server and interface information
- Whitelist information

To create a ScanSafe template, follow these steps:

**Step 1** Choose Configuration > Templates > Features & Technologies > Security > ScanSafe.

**Step 2** In the Template Basic area, enter a name and a description in the appropriate fields.

**Step 3** In the Validation Criteria area, choose a device type from the list and enter the OS version.

**Step 4** In the Template Detail area, enter the required information. For more information about the required field descriptions, see the Cisco Prime Infrastructure 3.1 Reference Guide.

**Step 5** Click Save as New Template. After you save the template, apply it to your devices using the procedures in Creating Feature-Level Configuration Templates.

Configuring Interfaces

The Interfaces feature helps in setting up physical and logical interfaces. Physical interfaces on a device depend on the device type and its interface processors or port adapters. IPv4 addressing is supported for all interfaces including service modules such as WAN, LAN, and logical interfaces. The following interfaces are supported in this release:

**WAN Interfaces**
- Configuring a Serial Interface
- Configuring POS Interface
- Configuring a Service Module
- Configuring Controllers

**LAN Interfaces**
- Creating a Gigabit Ethernet or Fast Ethernet Interface

**Logical Interfaces**
- Creating a Loopback Interface
- Creating a VLAN Interface
- Creating a Tunnel Interface
Configuring a Serial Interface

To edit or delete the Serial interface, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**.
Step 2 After choosing the device from list, click **Configuration**. The Feature Configuration pane appears.
Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.
Step 4 In the Interface page, select the serial interface in the Interface Summary area and click **Edit**.
Step 5 In the Create or Edit Serial Interface page, enter the basic configuration information.
Step 6 Select the encapsulation type as **High Level Data Link Control (HDLC)** or **Point-to-Point Protocol (PPP)** or **Frame Relay**. Use the Advance Configuration area to configure the encapsulations.

**Note** For controller-based serial interfaces, only interface configurations are supported.

Step 7 Enter an IPv4 address.
Step 8 For Frame Relay encapsulation, use the IETF option to connect to non-Cisco routers. (The Autosense feature is supported only on Frame Relay.)

**Note** The Autosense feature allows the router to detect the LMI type that is being used, by communicating with the switch and then uses the same type of LMI.

Step 9 For PPP encapsulation, specify the CHAP and PAP configurations with directions.
Step 10 Click **Save**. The Interface Summary page displays the modified interfaces.
Step 11 Click **Save** to save the changes in the device.

Configuring POS Interface

To edit and delete the POS interface, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**.
Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.
Step 3 In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.
Step 4 In the Interface page, select the POS interface from the Interface Summary area and click **Edit**.
Step 5 In the Create or Edit POS Interface page, enter the basic configuration information.
Step 6 Select the **Enable SPE Scrambling** check box to enable the SPE scrambling.
Step 7 Select the **Send LAIS when Shutdown** check box to send the Line Alarm Indication Signal (LAIS) when the POS interface is in administrative shut down state.
Configuring Interfaces

Step 8  Select the encapsulation type as HDLC or PPP or Frame Relay and use the Advance Configuration area to configure the encapsulations.

Step 9  Enter an IPv4 address.

Step 10  In the Advanced Configuration area, select the alarm reporting and alarm reporting threshold options to receive alarms when there is any event.

Step 11  Repeat Step 9 through Step 11 in the Configuring a Serial Interface area.

Configuring a Service Module

To edit or delete the Service Module interface, follow these steps:

Step 1  Choose Inventory > Device Management > Network Devices.

Step 2  After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3  In the Feature Configuration pane, expand the Interface folder, then click Interfaces.

Step 4  Select the service module interface from the Interface Summary area and click Edit.

Step 5  In the Fast Ethernet interface pane, complete the basic configuration information.

Step 6  Click OK to save the changes in the device.

Configuring Controllers

To create or edit the DSL, SHDSL, and VDSL controllers interface, follow these steps:

Step 1  Choose Inventory > Device Management > Network Devices.

Step 2  After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3  In the Feature Configuration pane, expand the Interface folder, then click Interfaces.

Step 4  Select the DSL, SHDSL or VDSL controller from the interface summary area and click Edit.

Step 5  In the Edit Controller page, enter the required information.

Step 6  Click OK. After you configure the controller, you must configure the DSL, SHDSL or VDSL subinterface.

Step 7  To configure the DSL subinterface, select an ATM interface in the Interface Summary page, and click Add Subinterface.

a. In the Create ATM Sub Interface page, choose the encapsulation from the drop-down list.

b. Configure the Permanent Virtual Circuit (PVC) settings.

c. Select a dialer to be associated to the ATM subinterface by using the Create or Associate dialer options.

d. Click OK.
Step 8 To configure the SHDL subinterface, select a SHDSL interface in the Interface Summary page, and click Add Subinterface.
   a. In the Create SHDSL subinterface page, add the DSL Group and select the DSL pair.
   b. Choose the Group Type from the drop-down list.
   c. Click OK.

Step 9 To configure the VDSL subinterface, select a VDSL interface in the Interface Summary area, and click Add Subinterface.
   a. In the Create VDSL subinterface page, choose the Operating Mode from the drop-down list.
   b. Select the Annex A mode check box.
   c. Click OK.

Creating a Gigabit Ethernet or Fast Ethernet Interface

To create a Gigabit Ethernet or Fast Ethernet interface, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.
Step 3 In the Feature Configuration pane, expand the Interface folder, then click Interfaces.
Step 4 Select the Gigabit Ethernet or Fast Ethernet in the Interface Summary area, and click Edit.
Step 5 In the Edit Ethernet Interface, complete the basic configuration information.
Step 6 Choose the Primary IP address from the drop-down list.
Step 7 Click Add Row and add the Secondary IP address.
Step 8 Click OK to save the changes in the device.

Creating a Loopback Interface

To create a Loopback interface, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.
Step 3 In the Feature Configuration pane, expand the Interface folder, then click Interfaces.
Step 4 On the Interface page, choose Add Logical Interface > Loopback.
Step 5 In the Create or Edit Loopback Interface area, enter the basic configuration information.
Step 6 Enter an IPv4 address.
Step 7 Click OK.
Step 8 Click Save to save the changes in the device.
Creating a VLAN Interface

To create a VLAN interface, follow these steps:

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  After choosing the device from the list, click Configuration. The Feature Configuration pane appears.
Step 3  In the Feature Configuration pane, expand the Interface folder, then click Interfaces.
Step 4  In the Interface page, click Add Logical Interface > VLAN.
Step 5  In the Create or Edit VLAN Interface page, complete the basic configuration information.
Step 6  Choose the Primary IP address from the drop-down list.
Step 7  Click Add Row and add the Secondary IP address.
Step 8  Click OK to save the changes in the device.

Editing a VLAN Interface

To edit the VLAN interface, follow these steps:

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  After choosing the device from the list, click Configuration. The Feature Configuration pane appears.
Step 3  In the Feature Configuration pane, expand the Interface folder, then click Interfaces.
Step 4  Select the VLAN interface from the Interface Summary area, and click Edit.
Step 5  In the Create or Edit VLAN Interface page, complete the basic configuration information.
Step 6  Choose the Primary IP address from the drop-down list.
Step 7  Click Add Row and add the Secondary IP address.
Step 8  Click OK to save the changes in the device.

Creating a Tunnel Interface

To create a Tunnel interface, follow these steps:

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  Choose the device from the list or click Add to create a new device, then configure the device.
Step 3  After choosing the device, choose Configuration. The Feature Configuration pane appears.
Step 4  Expand the Interface folder, then choose the Interfaces.
Step 5  In the Interface page, choose Add Logical Interface > Tunnel.
Step 6  In the Create or Edit Tunnel Interface page, complete the basic configuration information.
Step 7  Choose the Primary IP address from the drop-down list.
Step 8  Click **Add Row** and add the Secondary IP address.

Step 9  Click **OK** to save the changes in the device.

---

**Editing an Existing Tunnel Interface**

To edit a Tunnel interface, follow these steps:

---

**Step 1**  Choose **Inventory > Device Management > Network Devices**.

**Step 2**  After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

**Step 3**  In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

**Step 4**  Select the Tunnel interface in the Interface Summary page, and click **Edit**.

**Step 5**  In the Create or Edit Tunnel Interface page, complete the basic configuration information.

**Step 6**  Choose the Primary IP address from the drop-down list.

**Step 7**  Click **Add Row** and add the Secondary IP address.

**Step 8**  Click **OK** to save the changes in the device.

---

**Creating a Virtual Template Interface**

To create a Virtual Template interface, follow these steps:

---

**Step 1**  Choose **Inventory > Device Management > Network Devices**.

**Step 2**  After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

**Step 3**  In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

**Step 4**  In the Interface page, click **Add Logical Interface Virtual Template**.

**Step 5**  In the Create or Edit Virtual Template Interface page, complete the basic configuration information.

**Step 6**  Choose the Primary IP address from the drop-down list.

**Step 7**  Click **Add Row** and add the Secondary IP address.

**Step 8**  Click **OK** to save the changes in the device.

---

**Editing an Existing Virtual Template Interface**

To edit a Virtual Template interface, follow these steps:

---

**Step 1**  Choose **Inventory > Device Management > Network Devices**.

**Step 2**  After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

**Step 3**  In the Feature Configuration pane, expand the **Interface folder**, then click **Interfaces**.

---
Configuring Cellular WAN Interfaces

The Cisco ISRs provide a third-generation (3G) wireless interface that can be used over GSM and Code Division Multiple Access (CDMA) networks. Its primary application is WAN connectivity as a backup data link for critical data applications. However, the 3G wireless interface can also function as the primary WAN connection for the router. The 4G wireless interface is supported only on the 4G-LTE-V modem.

Configuring a CDMA Interfaces

To configure a CDMA interface, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Interface folder, then click Cellular WAN Interfaces.

Step 4 For a CDMA Sprint modem:
   a. Select a cellular interface with CDMA Sprint modem, and click Manage Modem.
   b. In the Manage Modem dialog box, select the OMA-DM or Manual radio button. If you choose the Manual option, complete the fields to manually configure the CDMA Sprint modem, then click OK.

Step 5 For a CDMA Verizon modem:
   a. Select a cellular interface with CDMA Verizon modem, and click Manage Modem.
   b. In the Manage Modem dialog box, enter the Account Activation Information, then click OK.

Step 6 For a CDMA Generic modem:
   a. Select a cellular interface with CDMA Generic modem, and click Manage Modem.
   b. In the Manage Modem dialog box, complete the fields to configure the CDMA Generic Modem, then click OK.

Configuring a GSM Interfaces

To configure a GSM interface, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 Choose the device from the list or click Add to add a new device, then configure the device.
Step 3 After choosing the device, click Configuration. The Feature Configuration pane appears.
Step 4 Expand the Interface folder, then choose Cellular WAN Interfaces.
Step 5 Select the GSM interface and click Manage Modem.
Step 6 In the Manage Modem dialog box, click Add Row.
Step 7 Choose the Profile Number from the drop-down list, and enter the Access Point Name, then click OK.

Configuring Network Address Translation (NAT)

Network Address Translation (NAT) is a process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. NAT helps to limit the number of public IP addresses used by an organization or company, for both economy and security purposes.

The NAT feature allows organizations to resolve the problem of IP address depletion when they have existing networks and need to access the Internet. NAT allows the IP network of an organization to use different IP address space for the outside network. Thus, NAT allows an organization that does not have globally routable addresses to connect to the Internet by translating those addresses into globally routable address space. NAT also allows a more graceful renumbering strategy for organizations that are changing service providers or voluntarily renumbering into Classless Inter Domain Routing (CIDR) blocks. NAT is described in RFC 1631.

A router configured with NAT will have at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit router between a subdomain and a backbone. When a packet leaves the domain, the NAT translates the locally significant source address into a globally unique address. When a packet enters the domain, NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. If NAT cannot allocate an address because it has run out of addresses, it drops the packet and sends an Internet Control Message Protocol (ICMP) host unreachable packet.

For more information on NAT, see IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S.

NAT Types

NAT operates on a router—generally connecting only two networks together—and translates your private (inside local) addresses within the internal network, into public (inside global) addresses before any packets are forwarded to another network. This functionality gives you the option to configure the NAT so that it will advertise only a single address for your entire network to the outside world. Doing this effectively hides the internal network from the world, giving you additional security.

NAT types include:

- Static Address Translation (SAT) — Allows one-to-one mapping between local and global addresses.
- Dynamic Address Translation (DAT) — Maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.
• Overloading—A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as Port Address Translation (PAT). With PAT, thousands of users can be connected to the Internet using only one real global IP address.

### Configuring NAT for IP Address Conservation

To configure NAT, perform the following steps:

1. **Creating NAT IP Pools** (required for Dynamic NAT)
2. Create an ACL template and configure the ACL
3. **Creating NAT44 Rules**
4. **Configuring Interfaces** and assign rules on them
5. **Setting Up NAT MAX Translation** (Optional)

---

**Note**
The NAT feature is supported on the following: ASR platform from Cisco IOS Release 3.5 or later and ISR platform from Cisco IOS Release 12.4(24)T or later.

**Caution**
CLI changes that begin with “EMS_” are not supported and might cause unexpected behavior.

### Creating NAT IP Pools

The IP Pool is a device object that represents IP ranges to be used with Dynamic NAT. The NAT IP Pools feature allows you to create a new pool that can be used with Dynamic NAT, change the existing pool, and delete the pool from the device.

To create an IP pool, follow these steps:

---

**Step 1** Choose **Inventory > Device Management > Network Devices**.

**Step 2** After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

**Step 3** In the Feature Configuration pane, expand the Security, expand the NAT subfolder, and then click IP Pools. The NAT Pools page appears.

**Step 4** Click **Add IP Pool > IP+Prefix** or **IP Range + Prefix**, and enter the Name, IP Address/Range, Prefix Length, and Description. You cannot change the name of the pool after creating the pool.

**Note**
A valid IPv4 address consists of 4 octets separated by a period (.).

**Step 5** Click **Save** to deploy the IP pool to the device, or **Cancel** to cancel your editing.

**Step 6** To edit the existing IP Pool, in the NAT IP Pools page do the following:

a. Click in the selected IP Pools parameters row, and edit the parameters. or

b. Select the IP Pools, and click **Edit**. The selected IP Pools opens for editing. You can edit all of the parameters except the pool name.
Creating NAT44 Rules

The NAT44 feature allows you to create, delete, and change NAT44 rules.
There are three types of NAT rules:

- Static
- Dynamic
- Dynamic PAT

To create the NAT44 rule, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**.
Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.
Step 3 In the Feature Configuration pane, expand the **Security**, expand the **NAT** subfolder, and then click **NAT44 Rules**.
Step 4 In the NAT 44 page, click the down arrow icon next to the **Add NAT Rule** button.
  - Click **Static** to create Static Rule. For a description of the elements, see the *Cisco Prime Infrastructure 3.1 Reference Guide*.
  - Click **Dynamic** to create Dynamic NAT Rule. For a description of the elements, see the *Cisco Prime Infrastructure 3.1 Reference Guide*.
  - Click **Dynamic PAT** to create Dynamic PAT Rule. For a description of the elements, see the *Cisco Prime Infrastructure 3.1 Reference Guide*.
Step 5 Click **Save** to save and deploy the changes to the device.
Step 6 To edit the existing NAT44 rule in the NAT44 page, do one of the following:
  - Click the selected NAT44 rules parameters row, and edit the parameters.
  - Select the NAT44 rule, and click **Edit**. The selected NAT44 rule opens for editing. You can edit all of the parameters.
Step 7 You can change the Source and Destination according to the creation rules. You can also change the Options selection according to the creation rules.
Step 8 Click **Save** to save the changes in the server.

Configuring Interfaces

A virtual interface is a logical interface configured with generic information for a specific purpose or for specific users, plus router-dependent information.

To configure a virtual interface, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**.
Step 2 After choosing the device from list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security, expand the NAT subfolder, and then click Interfaces.

In the Interface page, select the interface that you want to change and choose the association from the drop-down list. The options are: Inside, Outside, and None.

Step 4 Click Save to save the changes in the server.

---

Setting Up NAT MAX Translation

The NAT MAX Translation feature provides the ability to limit the maximum number of concurrent NAT operations on a router. In addition, the NAT MAX feature gives users additional control to use the NAT addresses. The Rate Limiting NAT Translation feature can be used to limit the effects of viruses, worms, and denial-of-service attacks. For more information on Configuring the Rate Limiting NAT Translation Feature, see Configuring NAT for IP Address Conservation in IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S.

The NAT MAX Translation feature allows you to reset the global translation attribute values.

To set up the MAX Translation, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Choose the device from the list or click Add to create a new device, then configure the device.

Step 3 After choosing the device, click Configuration. The Feature Configuration pane appears.

Step 4 Expand the Security, expand the NAT subfolder, and then click Advanced Settings > Max Translation.

Step 5 Reset the parameter values. Configure the maximum number of NAT entries that are allowed for all of the parameters. A typical range for a NAT rate limit is from 100 to 300 entries.

Step 6 Click Save to save the changes in the server.

---

Configuring DMVPN

The DMVPN feature allows you to scale large and small IP Security (IPsec) VPNs by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).

A typical VPN connection is a point-to-point IPsec tunnel connecting two routers. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes, using a GRE over an IPsec tunnel. IPsec traffic is routed through the hub to the spokes in the network.

See Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs) for more information about DMVPN (requires a Cisco.com login ID).

Cisco Network Control System allows you to configure your router as a DMVPN hub, DMVPN spoke or cluster. You can configure the router in the following ways:

- Configuring Hub and Spoke Topology
- Configuring a DMVPN Fully Meshed Topology
Creating a DMVPN Tunnel

To create a DMVPN tunnel, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.
Step 3 In the Feature Configuration pane, expand the Security folder, and then click DMVPN. Click Add to create the DMVPN.
Step 4 In the Device Role and Topology Type area, select the topology and the device role. The options are: Spoke, Hub, and Dynamic Connection between Spokes.
Step 5 In the Multipoint GRE Interface Information area, choose the WAN interface that connects to the Internet from the drop-down list.
Step 6 Enter the IP address of the Tunnel Interface, and Subnet Mask.
Step 7 Complete the fields in the NHRP and Tunnel Parameters area.

Note The Network ID is a unique 32-bit network identifier from a Non Broadcast Multiaccess (NBMA) network. The tunnel key is used to enable a key ID for a particular tunnel interface. The MTU size of IP packets that are sent on a particular interface.

Note The default MTU value for Ethernet and the serial interface is 1500. The default value varies depending upon the media type. The Tunnel throughput delay is used to set the delay value for a particular interface.

Step 8 In the Encryption policy field, click the anchored plus button (+) to add the Transform Set Profile (see Security > VPN Components > Transform Sets in the Cisco Prime Infrastructure 3.1 Reference Guide).
Step 9 In the Transform Set Profile dialog box, enter the Name and choose the acceptable combination of security protocols and algorithm from the drop-down list to configure the transform set.
Step 10 Select the IP Compression check box to enable the IP compression for the transform set.
Step 11 Choose the mode for the transform set. The options are: Tunnel mode or Transport mode.
Step 12 In the NHS Server Information area, enter the IP address for the physical interface of the hub and tunnel and the Fallback Time. If the device supports the cluster then add the next hop server information, such as Cluster ID, Max Connection, Hub IP address, and Priority.

Note The NHS server information is required only for spoke configuration. If you select the Use Cluster for NHS check box, add the information, such as Cluster ID, Max Connection, and Next Hub Server. The template with the NHS cluster configuration will be applied only to the device running Cisco IOS Software Release 15.1(2)T or later.

Step 13 In the Routing Information area, choose the routing information. The options are: EIGR, RIPV2, and Other.
Note The routing information is required only for hub configuration.

Step 14 Choose the existing EIGRP number from the drop-down list or enter an EIGRP number. Use the Other option to configure the other protocols.

Step 15 Click Save to save the single NHS server entry details and the priority of the server, save the entire group of server, and save the NHS cluster information. When you save the NHS cluster information, the NHS server will be populated in the non-editable field.

Step 16 Click OK to save the configuration to the device.

Configuring Hub and Spoke Topology

To configure the hub and spoke topology, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security folder, and then click DMVPN. Click the Add button to create the DMVPN tunnel.

Step 4 In the Device Type and Topology area, choose Hub and Spoke as the topology, and select either Hub or Spoke as a device role.

Step 5 Choose the WAN interface from the drop-down list, and then configure the Multipoint GRE IP Address and the subnet mask for the tunnel interface.

Step 6 Configure the NHRP and the Tunnel Interface parameters, such as the IP address, NHRP parameters and map, MTU value, Source of the Tunnel, Tunnel Mode, and Tunnel Key.

Step 7 Create the transform-set for protecting the data flow between the devices. You can specify up to four transforms: One Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IPsec protocols and the algorithms.

Step 8 Configure the routing protocol to be used.

Step 9 Click Save to save the configuration to the device.

Configuring a DMVPN Fully Meshed Topology

The dynamic spoke-to-spoke option allows you to configure a DMVPN fully meshed topology. In this topology, you can configure the router as a spoke, capable of establishing a directIPsec tunnel to other spokes in the network.

To configure a DMVPN Fully Meshed topology, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Choose the device from the list or click Add to create a new device, then configure the device.
Step 3 After selecting the device, click Configuration. The Feature Configuration pane appears.

Step 4 Expand the Security folder, and then click DMVPN. Click the Add to create the DMVPN tunnel with fully meshed topology.

Step 5 In the Create DMVPN Tunnel configuration page, select the Full Mesh radio button to configure the network type as full mesh topology.

Step 6 Repeat Step 6 through Step 8 in the Configuring Hub and Spoke Topology section.

Step 7 For Fully Mesh spoke topology, in the NHS Server Information area, add the next hub server information, such as the IP Address of Hub’s physical interface and the IP address of Hub’s tunnel interface.

Step 8 Click Save to save the configuration to the device.

Configuring a Cluster Topology

To configure a cluster topology, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 Feature Configuration pane, expand the Security folder, and then click DMVPN. Click Add to create the DMVPN tunnel.

Step 4 From the Create DMVPN Tunnel configuration page, select Spoke radio button to configure the device role as a spoke.

Step 5 Repeat Step 6 through Step 8 from in the Configuring Hub and Spoke Topology section.

Note The device must be running IOS version of 15.1(2)T or later.

Step 6 Click Add Row to configure the cluster related information, and add the Cluster-ID and Maximum Connection values.

Step 7 Click Expand Row (next to the radio button) and click Add Row to add the NHS server information.

Step 8 Enter the NHS server, the GRE Tunnel IP addresses, and the Priority of this NHS server. Click Save to save the NHS server entry configuration.

Step 9 Click Save to save the NHS server group information.

Step 10 Click Save again to save the NHS group information with the cluster configuration. This will automatically populate the NHS server IP address in the table.

Editing a DMVPN

To edit a DMVPN tunnel, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
**Configuring GETVPN**

A Group Encrypted Transport VPN (GETVPN) deployment has three primary components: Group Member, Key Server, and Group Domain of Interpretation protocol. Group Members encrypt and decrypt the traffic, and Key Server distributes the encryption key to all group members. The Key Server decides on a single data encryption key for a given lifetime. Because all Group Members use the same key, any Group Member can decrypt the traffic encrypted by any other Group Member. GDOI protocol is used between the Group Member and Key Server for group key and group Security Association (SA) management. A minimum one Key Server is required for a GETVPN deployment.

Unlike traditional IPsec encryption solutions, GETVPN uses the concept of group SA. All members in the GETVPN group can communicate with each other using a common encryption policy and a shared SA. Therefore, there is no need to negotiateIPsec between Group Members on a peer-to-peer basis, thereby reducing the resource load on the Group Member routers.

---

**Deleting a DMVPN**

To delete a DMVPN tunnel, follow these steps:

1. Choose Inventory > Device Management > Network Devices.
2. Choose the device from the list to delete the DMVPN tunnel. If the device is not added, click Add to add the device.
3. After selecting the device, click Configuration. The Feature Configuration pane appears.
4. Expand the Security folder, and then click DMVPN. The available tunnel is displayed.
5. Select the tunnel, and click Delete.
6. Click Yes on the warning message to delete the selected tunnel.
7. Click No on the warning message if you do not want to delete the selected tunnel.
8. Click Cancel to cancel all of the changes that you have made without sending them to the router.

---

**Configuring GETVPN**

A Group Encrypted Transport VPN (GETVPN) deployment has three primary components: Group Member, Key Server, and Group Domain of Interpretation protocol. Group Members encrypt and decrypt the traffic, and Key Server distributes the encryption key to all group members. The Key Server decides on a single data encryption key for a given lifetime. Because all Group Members use the same key, any Group Member can decrypt the traffic encrypted by any other Group Member. GDOI protocol is used between the Group Member and Key Server for group key and group Security Association (SA) management. A minimum one Key Server is required for a GETVPN deployment.

Unlike traditional IPsec encryption solutions, GETVPN uses the concept of group SA. All members in the GETVPN group can communicate with each other using a common encryption policy and a shared SA. Therefore, there is no need to negotiateIPsec between Group Members on a peer-to-peer basis, thereby reducing the resource load on the Group Member routers.
**Group Member**

The Group Member registers with the Key Server to get the IPsec SA that is necessary to encrypt data traffic within the group. The Group Member provides the group identification number to the Key Server to get the respective policy and keys for this group. These keys are refreshed periodically by the Key Server, before the current IPsec SAs expire, so that there is no traffic loss.

**Key Server**

The Key Server is responsible for maintaining security policies, authenticating Group Members and providing a session key for encrypting traffic. Key Server authenticates the individual Group Members at the time of registration. Only after successful registration can the Group Members participate in a group SA.

A Group Member can register at any time and receive the most current policy and keys. When a Group Member registers with the Key Server, the Key Server verifies the group identification number of the Group Member. If this identification number is valid, and the Group Member has provided valid Internet Key Exchange (IKE) credentials, the Key Server sends the SA policy and the keys to the group member.

The keys sends two types to Group Member: the Key Encryption Key (KEK) and the Traffic Encryption Key (TEK). The TEK becomes part of the IPsec SA with which the group members within the same group encrypt the data. The KEK is used to secure rekey messages between the Key Server and the Group Members.

The Key Server sends out rekey messages either because of an impending IPsec SA expiration or because the security policy has changed on the Key Server. Keys can be distributed during rekey using either multicast or unicast transport. the multicast method is more scalable because keys need not be transmitted to each group member individually. Unlike in unicast, The Key Server will not receive acknowledgment from the Group Member about the success of the rekey reception using the multicast rekey method. Using the unicast rekey method, the Key Server will delete a Group Member from its database if the Group Member does not acknowledge three consecutive rekeys.

**Group Domain of Interpretation**

Group Domain of Interpretation protocol is used for Group key and group SA management. Group Domain of Interpretation uses Internet Security Association Key Management Protocol (ISAKMP) for authenticating the Group Members and Key Servers. All of the standard ISAKMP authentication schemes like RSA Signature (certificates) and preshared key can be used for GETVPN.


**Creating a GETVPN Group Member**

Use the Add GroupMember configuration page to configure a GETVPN group member.

To create a GETVPN group member, follow these steps:

**Step 1** Choose **Inventory > Device Management > Network Devices**.

**Step 2** After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

**Step 3** In the Feature Configuration pane, expand the **Security** folder, and then click **GETVPN-GroupMember**. Click **Add** to create the GET VPN group member.

**Step 4** In the Add GroupMember dialog box, choose the **General** tab, and enter the Group Name and Group Identity. Choose the Registration Interface from the drop-down list.
Enter the Primary Key Server and Secondary Key Server IP addresses. Click Add Row or Delete to add or delete the secondary key server IP addresses.

**Note** The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizes with the secondary key servers. The server with the highest priority is elected as a primary key server.

Click the row or field to edit the secondary key server IP address. Click Save to save the configuration.

In the Add Group Member dialog box, choose the Advanced tab, and choose the Local Exception ACL and Fail Close ACL from the drop-down list.

If the Fail Close feature is configured, all of the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.

Choose the Migration tab, and select the Enable Passive SA check box to enable passive SA. Use this option to turn on the Passive SA mode for this group member.

Click OK to add the Group member in the table. To display the commands, click CLI preview. After the scheduled deploy is completed, the configuration is applied on the device.

### Creating a GETVPN Key Server

Use the Add KeyServer configuration page to configure the GETVPN key server.

To create a GETVPN key server, follow these steps:

Choose Inventory > Device Management > Network Devices.

After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

In the Feature Configuration pane, expand the Security folder, and then click GETVPN-KeyServer.

Click Add to create the GETVPN key server.

In the Add Key Server dialog box, choose the General tab, and enter the Group Name, Group Identity, WAN IP address, and Priority of this key server.

Enter the Co-operative Key Servers IP address. Click Add Row or Delete to add or delete the Co-operative key server IP address. Click the row or field, and edit the IP address.

In the Add KeyServer dialog box, choose the Rekey tab, and choose the Distribution method from the drop-down list.

The distribution method is used to send the rekey information from key server to group members. When you choose the distribution method as multicast, specify the multicast address to which the rekey needs to be transmitted.

In the Add KeyServer dialog box, choose the GETVPN Traffic tab, and enter the Traffic to be encrypted, Encryption Policy, and Anti Replay.

The access list defines the traffic to be encrypted. Only the traffic which matches the “permit” lines will be encrypted. Be sure not to encrypt certain traffic that should always be permitted even if the crypto sessions are not active.
Step 8  Click OK to add the Group member in the table. To display the commands, click CLI preview. After the scheduled deployment is completed, the configuration is applied on the device.

Editing a GETVPN Group Member or Key Server

To edit a GETVPN group member or a GETVPN key server, follow these steps:

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  After choosing the device from the list, click Configuration. The Feature Configuration pane appears.
Step 3  In Feature Configuration pane, expand the Security folder, and then click GETVPN-Group Member or GETVPN-KeyServer. The GETVPN-GroupMember or GETVPN-KeyServer summary page opens.
Step 4  In the GETVPN summary page, select the group name and click Edit. The Edit GETVPN-GroupMember or GETVPN-Keyserver page appears.
Step 5  In the Edit GETVPN-GroupMember or GETVPN-KeyServer page, you can edit the GETVPN parameters.
Step 6  Click OK to save the configurations.

Deleting a GETVPN Group Member or Key Server

To delete a GETVPN group member or GETVPN key server, follow these steps:

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  Choose the device from the list or click Add to add a new device, then configure the device. The device details appear on the lower part of the page.
Step 3  After choosing the device, click Configuration. The Feature Configuration pane appears.
Step 4  In the Feature Configuration pane, expand the Security folder, and then click GETVPN-Group Member or GETVPN-KeyServer. The GETVPN-GroupMember or GETVPN-KeyServer summary page opens.
Step 5  In the GETVPN summary page, select the group name and click Delete.
Step 6  Click OK to save the configurations.

Configuring VPN Components

The Internet Key Exchange (IKE) is a standard method for arranging secure and authenticated communications. The IKE establishes session keys (and associated cryptographic and networking configuration) between two hosts across network. IKE policies protect the identities of peers during authentication.
IKE negotiations must be protected; therefore, each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states the security parameters that will be used to protect subsequent IKE negotiations. After the peers agree on a policy, the security parameters of the policy are identified by a security association established at each peer. These security associations are applied to all subsequent IKE traffic during the negotiation.

When negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates negotiation sends all of its policies to the remote peer. The remote peer looks for a match by comparing its own highest priority policy against the other peer’s received policies. A match is found when policies from both peers contain the same encryption, hash, authentication, and Diffie-Hellman (D-H) parameter values, and when the remote peer’s policy specifies a lifetime that is less than or equal to the lifetime of the policy it is being compared to. If the lifetimes are not identical, the shorter lifetime from the remote peer’s policy is used.

The VPN components primarily include the following:

- Configuring IKE Policies
- Configuring IKE Settings
- Configuring IPsec Profiles
- Creating Preshared Keys
- Creating RSA Keys
- Configuring Transform Sets

### Configuring IKE Policies

To configure IKE policies, follow these steps:

1. Choose **Inventory > Device Management > Network Devices**.
2. After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.
3. In the Feature Configuration pane, Expand the **Security** folder, and then choose **VPN Components > IKE Policies**.
4. Click **Add Row** to create the IKE policies.
5. In the IKE Policies page, enter the Priority, Authentication, D-H Group, Encryption, Hash, and Lifetime.

   For a description of the elements on the IKE Policies page, see Security > VPN Components > IKE Policies in the *Cisco Prime Infrastructure 3.1 Reference Guide*.

6. Click **Save** to save the configuration, then click **Save** again to generate the CLI commands.

### Configuring IKE Settings

The IKE Settings feature allows you to globally enable IKE for your peer router.

To configure IKE settings, follow these steps:

1. Choose **Inventory > Device Management > Network Devices**.
2. After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.
Step 3 In the Feature Configuration pane, expand the **Security** folder, and then choose **VPN Components > IKE Settings**.

Step 4 Select the **Enable IKE** and **Enable Aggressive Mode** check box to enable the IKE policies and the aggressive mode.

Step 5 Choose the IKE Identity from the drop-down list.

Step 6 Enter the **Dead Peer Detection Keepalive** and **Dead Peer Detection Retry** time in seconds.

For a description of the elements on the IKE Settings page, see Security > VPN Components > IKE Settings in the *Cisco Prime Infrastructure 3.1 Reference Guide*.

Step 7 Click **Save** to save the configuration.

---

### Configuring IPsec Profiles

The IPsec profiles, also called ISAKMP profiles, enable you to define a set of IKE parameters that you can associate with one or more IPsec tunnels. An IPsec profile applies parameters to an incoming IPsec connection identified uniquely through its concept of matching identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, Fully Qualified Domain Name (FQDN), and group the VPN remote client grouping.

The IKE Profile feature allows you to create an IPsec profile.

Step 1 Choose **Inventory > Device Management > Network Devices**.

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the **Security** folder, and then choose **VPN Components > IPsec Profile**.

Step 4 Click **Add Row** to create the IPsec profile.

Step 5 In the IPsec Profile page, enter the information such as Name, Description, and Transform Set, and the IPsec SA Lifetime.

**Note** When you edit a profile, you cannot edit the name of the IPsec profile. A transform set represents a certain combination of security protocols and algorithms. During the IPsec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform describes a particular security protocol with its corresponding algorithms.

Step 6 Enter the IPsec SA Lifetime in seconds to establish a new SA after the set period of time elapses.

Step 7 To edit the IPsec profile parameters, click **Field** and edit the parameter of that IPsec profile.

Step 8 To delete the IPsec profile, select the IPsec Profile from the list, and click **Delete**.

Step 9 Click **Save** to save the configuration, then click **Save** again to generate the CLI commands.
Creating Preshared Keys

The preshared Keys feature allows you to share a secret key between two peers. This key is used by the IKE during the authentication phase.

To create a preshared key, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 Select a device or click Add to add a new device, and then configure the device. The device details appear in the lower part of the page.
Step 3 After selecting the device, click Configuration. The Feature Configuration pane appears.
Step 4 Expand the Security folder, and then choose VPN Components > Preshared Keys.
Step 5 Click Add Row to create the preshared key.
Step 6 In the Preshared Keys page, enter the IP Address, Host Name, Subnet Mask, and Preshared Keys.
Step 7 To edit the preshared key parameters, click the Field and edit the parameter of that preshared key.
Step 8 To delete the preshared key, choose the preshared key from the list, and click Delete.
Step 9 Click Save to save the configuration, then click Save again to generate the CLI commands.

Creating RSA Keys

An RSA key pair consists of a public key and a private key. When setting up your Public Key Infrastructure (PKI), you must include the public key in the certificate enrollment request. After the certificate is granted, the public key is included in the certificate so that peers can use it to encrypt the data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by the peers and to digitally sign transactions when negotiating with the peers.

RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, it takes longer to generate, encrypt, and decrypt keys with large modulus values.

To create an RSA keys, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.
Step 3 In the Feature Configuration pane, expand the Security folder, and then choose VPN Components > RSAKeys.
Step 4 Click Add Row to create the RSA keys.
Step 5 The Add RSA Keys dialog box appears.
Step 6 In the Add RSA Keys dialog box, enter the Label, Modulus, and Type.
Step 7 Select the **Make the Key exportable** check box to generate the RSA as a exportable key.

Step 8 Click **OK** to save the configuration.

Step 9 To import the RSA key, click **Import**. The Import RSA Key dialog box appears.

Step 10 In the Import RSA Key dialog box, enter the label of the RSA key, Key type, and password to decrypt the key. If the key type is general-keys, signature or encryption, copy and paste the public and private key data that was saved.

Step 11 To import usage-key, enter the public and private key data of both the signature and encryption keys.

Step 12 Click **Import** to import the RSA key.

Step 13 To export the RSA key, choose the RSA key from the list and click **Export**. The Export RSA Key Pair dialog box appears.

Step 14 In the Export RSA Key Pair dialog box, enter the password to encrypt the RSA key and choose the encryption algorithm from the drop-down list.

Step 15 Click **OK** to display the exported keys.

Step 16 To delete the RSA key, choose the RSA key from the list, and click **Delete**.

---

**Configuring Transform Sets**

To define a transform set, specify one to three transforms. Each transform represents an IPsec security protocol (AH or ESP) plus the algorithm that you want to use. When the particular transform set is used during negotiations for IPsec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

To configure a transform sets, follow these steps:

Step 1 Choose **Inventory > Device Management > Network Devices**.

Step 2 After choosing the device from the list, click **Configuration**. The Feature Configuration pane appears.

Step 3 **In the** Feature Configuration pane, expand the **Security** folder, and then choose **VPN Components > Transform Sets**.

Step 4 Click **Add Row** to create the transform sets.

Step 5 In the Transform Sets page, enter the Name and select the acceptable combination of security protocols and algorithm to configure the transform set.

Step 6 Specify the mode for a transform set:

---

**Note** The ESP encryption algorithm is used to encrypt the payload and the integrity algorithm is used to check the integrity of the payload.
Transport—Encrypt data only. Transport mode is used when both endpoints support IPsec. Transport mode places the authentication header or encapsulated security payload after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets.

Tunnel—Encrypt data and IP header. Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as a router to act as an IPsec proxy for multiple VPN users; tunnel mode should be used in those configurations.

Step 7 Click **Save** to save the configuration, then click **Save** again to save the configuration changes.

---

## Creating a Zone-Based Firewall

The Zone-Based Firewall feature allows you to easily manage Cisco IOS unidirectional firewall policy between groups of interfaces known as *zones*.

A zone is a group of interfaces that have similar functions or features. For example, on a router, Gigabit Ethernet interface 0/0/0 and Gigabit Ethernet interface 0/0/1 may be connected to the LAN. These two interfaces are similar because they represent the internal network, so they can be grouped into a zone for firewall configurations.

By default, the traffic between interfaces in the same zone is not subjected to any policy. The traffic passes freely.

When an interface is a member of a security zone, all traffic to and from that interface (except traffic going to the router or traffic going to another interface on the same zone) is dropped.

To permit traffic between interfaces that belong to different zones, a firewall policy with concrete rules must be pushed to the device. If the policy permits the traffic between these two zones (through inspect or pass actions) traffic can flow through the zones. **Figure 50-1** describes the security zone.

![Security Zone Diagram](image)

The following describe the relationships between the interfaces and security zones shown in **Figure 50-1**.

- Interfaces E0 and E1 are members of the security zone Z1.
- Interface E2 is a member of the security zone Z2.
- Interface E3 is not a member of any of the security zone.
In this scenario, the following situations exist:

- Traffic flows freely between interfaces E0 and E1 because they are members of the same security zone (Z1).
- If no policies are configured, traffic will not flow between zones (for example, E0 and E2, E1 and E2, E3 and E1, and E3 and E2).
- Traffic can flow between interface E0 or E1 and E2 only when an explicit policy is configured to permit the traffic between zone Z1 and zone Z2.

Traffic can never flow between E3 and interface E0, E1 or E2 because E3 is not a part of any security zone.

Prime Infrastructure supports the zone-based firewall feature on Cisco ASR, ISR, and CSR routers. Using Prime Infrastructure, you can configure a zone-based firewall policy template and deploy it to multiple devices. After you deploy the zone-based configuration, you can navigate to the Device Work Center to view the deployed firewall configuration on a specific device.

To monitor the zone-based firewall, check the Zone-Based Firewall Monitor Hits capability on the Device Work Center or the Prime Infrastructure syslog feature, which supports zone-based firewall syslog messages.

Prime Infrastructure can configure Zone-Based Firewall either through CLI (over Telnet or SSH) or through WSMA. Zone-Based Firewall can be configured through WSMA in a more efficient and robust method and we recommend that you use the WSMA protocols for configuring Zone-Based Firewall. For more information on using WSMA with Prime Infrastructure, see Configuring the Device using WSMA.

### Configuring a Zone-Based Firewall Template

To configure a zone-based firewall on more than one device, use a zone-based template to make the changes. For zone-based firewall templates, you must first design the zone-based firewall in the network by defining the zones in the network. In Prime Infrastructure, zones are represented by interface role global object, which dynamically selects the list of interfaces that belong to the zone. Next, define and create network objects in the firewall environment. The Zone-based firewall feature supports only IPv4 network in Prime Infrastructure. (IPv6 is not supported.)

**Note**

The Zone-Based Firewall feature is supported on the following: ASR platform from Cisco IOS-XE Release 15.2(2)S or later, ISR G2 platform from Cisco IOS Release 15.0(1)M or later, ISR G3 platform from Cisco IOS-XE 15.3(2)S Release or later, and CSR platform from Cisco IOS-XE 15.3(1)S Release or later.

To configure a zone-based firewall template:

1. Define the zones. A security zone is defined as an interface role (see Creating an Interface Role).
2. Define the IPv4 network objects (see Creating an IPv4 Network Object).

**Note** Cisco Prime Infrastructure 2.0 supports only IPv4 network objects.

3. Design a firewall policy and deploy it to multiple devices (for more information, see Creating a Policy Rule).
4. Validate the configuration for a specific device (see Creating a Zone-Based Firewall).
5. Modify the global objects and template configuration (see Creating a Zone-Based Firewall Policy Rules Template).


7. Monitor the syslog messages (for more information, see Viewing Syslogs).

To modify security zones, IPv4 network objects, and firewall policies, edit the firewall policy and redeploy it to the relevant devices.

Creating an Interface Role

An Interface role allows you to dynamically select a group of interfaces without having to manually define explicitly interfaces on each device. For example, you can use interface roles to define the zones in a zone-based firewall configuration template. You might define an interface role with a naming pattern of DMZ*. When you include this interface role in a template and deploy the template, the configuration is applied to all interfaces whose names begin with “DMZ” on the selected devices. As a result, you can, for example, assign a policy that enables anti-spoof checking on all DMZ interfaces to all relevant device interfaces with a single action.

For information to create an interface role, see Creating an Interface Role.

Creating an IPv4 Network Object

Network objects are logical collections of IP addresses or subnets that represent networks. Using network objects simplifies policy management.

For information to create an IPv4 network object, see Creating Network Objects.

Defining Device Override

Use the device override feature when a specific device is differed from the general network design.

To define the device override, follow these steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Configuration &gt; Templates &gt; Shared Policy Objects &gt; Shared &gt; Interface Role or IPv4 Network Object.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Create/Edit Network Object or Interface Role page, select the Allow Value Override Per Device check box and define the values per specific device. The defined values will override the regular values defined for the Interface Role \ Network Object.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click OK to save the configurations.</td>
</tr>
</tbody>
</table>

Creating a Zone-Based Firewall Policy Rules Template

After you create a shared policy objects, create a zone-based firewall policy rules template.

To create a Zone-Based Firewall Policy Rules template, follow these steps:
Chapter 50  Configuring Application Visibility and Control

Creating a Zone-Based Firewall

Step 1  Choose Configuration > Templates > Features & Technologies > Security > Zone Based Firewall > Policy Rules.

Step 2  In the Template Basic area, enter a name and a description in the appropriate fields.

Step 3  In the Validation Criteria area, choose a Device Type from the list and enter the OS Version.

Step 4  Enter the required fields. For descriptions of the template parameters, see the Cisco Prime Infrastructure 3.1 Reference Guide.

Step 5  Click Save as New Template. After you save the template, deploy it to your devices using the procedures in Creating Feature-Level Configuration Templates.

Configuring a Zone-Based Firewall on a Single Device

To configure a zone-based firewall on a single device, use Device Work Center zone-based configuration to make the changes.

Creating a Security Zone

To create a security zone, follow these steps:

Note

The Zone Based Firewall feature is supported on the ASR platform on Cisco IOS-XE Release 15.2 (2)S or later, ISR G2 platform on Cisco IOS release 15.0 (1) M or later, ISR G3 platform on Cisco IOS-XE Release 15.3(2)S or later, and CSR platform on Cisco IOS-XE Release 15.3(1)S.

Step 1  Choose Inventory > Device Management > Network Devices, then select a device.

Step 2  In the Feature Configuration pane, expand the Security subfolder.

Step 3  In the Security subfolder, expand the Zone Based Firewall > Common Building Blocks, and then click Zones.

Step 4  Click Add Zone to create the security zone.

Step 5  Select a Zone Name.

Step 6  Select the VRF of the zone.
   a. Select a VRF before assigning interfaces to the security zone. Only the interfaces that are assigned to the selected VRF can be assigned to the zone.
   b. If the user selects the “global VRF”, only interfaces which are not assigned to any VRF can be assigned to the zone.

Step 7  To assign the interfaces to the security zone, click the down arrow icon. The Interface Object Selector dialog box appears.
   a. In the Interface selector dialog box, select the Interface check box to select the interface from the list (can be multiple selection).
   b. Click OK to save the configuration or click Cancel to cancel all of the changes that you have made without sending them to the router.

Step 8  In the Advanced options column, click Configure. The Advanced Parameters Configuration dialog box appears.
Step 9 Define a set of advanced parameters which would be applicable for the inspected traffic that goes through the interfaces that belongs to the zone. For each parameter, select the check box to the left of the parameter name to override the default value for the parameter and then select the new value for the parameter. (Optional) In the Advanced Parameters Configuration dialog box, do the following:

<table>
<thead>
<tr>
<th>Note</th>
<th>Advanced Parameters option is supported only on ASR1K series devices.</th>
</tr>
</thead>
</table>

- a. Select the Alert check box and select the On radio button to set the alert.
- b. Select the Maximum Destination check box to set the maximum destination.
- c. Select the TCP SYN-Flood Rate per Destination check box to set the TCP flood rate.
- d. Select the Basic Threat Detection Parameters check box and select the On radio button to configure the FW drop threat detection rate, FW inspect threat detection rate, and FW SYN attack threat detection rate.

Step 10 Click:
- OK to save the configuration.
- Cancel to exit without saving.

Step 11 To edit the existing security zone parameters, select the zone, and click Edit in the Advance options column. The Advanced Parameters Configuration dialog box appears.

Step 12 In the Advanced Parameters Configuration dialog box, edit the values and click Save to save the changes. When you hover your mouse over the Advanced Options icon, the configured parameters will be displayed in the quick view window.

Step 13 Enter the description for the zone, then click Save.

---

**Editing a Security Zone**

To edit a security zone, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices, then select a device.

Step 2 In the Feature Configuration pane, expand the Security subfolder.

Step 3 In the Security subfolder, expand the Zone Based Firewall > Common Building Blocks, and then click Zones.

Step 4 In the Zones page, choose one of the following options:
- a. Click the Zone parameters row, and edit the parameters. or
- b. Select the zone, and click Edit. The selected Zone entity opens for editing.

Step 5 Click the add icon to assign the interface to the zone or to un-assign the existing interfaces from the zone. You can also change the Description of the zone and edit the advanced parameters of the zone.

Step 6 Click Save to save the configuration.
Configuring a Default-Zone

A default zone is a zone that is automatically assigned to all interfaces that are not assigned to any other zone on device.

To configure a default zone, follow these steps:

Note
The Default-Zone feature is supported only on the ASR platform.

Step 1
Choose Inventory > Device Management > Network Devices, then select a device.

Step 2
From the Feature Configuration pane, expand the Security subfolder.

Step 3
From the Security subfolder, expand the Zone Based Firewall > Common Building Blocks, and then click Zones.

Step 4
In the Zones page, click Enable Default to enable or disable the default security zone in the device. The default zone will host all of the interfaces that are not related to any zone.

Step 5
Click OK to save the configuration.

Creating a Policy Rule

To create a policy rule, follow these steps:

Step 1
Choose Inventory > Device Management > Network Devices, then select a device.

Step 2
In the Feature Configuration pane, expand the Security subfolder.

Step 3
In the Security subfolder, expand the Zone Based Firewall and then click Policy Rules. The Policy Rules page appears.

Step 4
From the Policy Rules page, click Add Rule and complete the fields. When you add a rule, you can place a rule at the top or bottom of the policy or after/before an existing rule. Firewall Rules are processed according to their order. To control the order of the rules, select the location of the rule in the table and use Add Top or Add Bottom option to add the rule to the top or the bottom of the table. Select a rule and use Add After or Add Before option to add the rule before or after an existing rule. You can place a rule at any given location and later use drag and drop to change its location.

Step 5
(Optional) Enter the firewall rule name. If you do not provide the name for the firewall rule, the system generates a name for the firewall rule. You cannot use these formats rule_<number> or EMS_rule_<number> to create the firewall rule name (For example, rule_1). These are system reserved formats.

Step 6
Select the source and destination zones for the rule, the rule is applicable only for traffic that flows from the source zone to the destination zone. Note that the source and destination zones must be different.

Step 7
To add the source and the destination IP address, click the add icon. The Source/Destination IP address dialog box appears.

a. In the Source/Destination IP address dialog box, select the Any check box to set the value to any.

b. Enter the Source/Destination IP addresses.

c. Click the + button to add the new IP address and the subnet.

d. Click the - button to remove an IP/subnet.
Creating a Zone-Based Firewall

e. Click OK to save the configurations or click Cancel to cancel all of the changes that you have made without sending them to the router.

Step 8 (Optional) Set the Service values. To add or remove the service, click the down arrow icon. The Firewall Service dialog box appears. You can also select a predefined Service. For creating services, see Creating a Service Group.

a. In the Firewall Service dialog box, select the service or port-based application check box to select the application or the service for the rule.

b. Select specific TCP/UDP ports by selecting TCP or UDP, close the window and enter the list of ports to be used in the text box that appears next to the TCP or UDP icon. For viewing port-based applications, see Assigning TCP/UDP Ports on an Application.

c. Use the navigation arrow buttons to navigate backward.

d. Click OK to save the configurations.

Step 9 Select the appropriate action. The options are: Drop, Drop and Log, Inspect, Pass, and Pass and Log.

Step 10 If you select the action to inspect, click Configure in the Advance options column. The Advanced Parameters Configuration dialog box appears.

Step 11 In the Advanced Parameters Configuration dialog box, do the following:

a. To customize the device default value, select the Parameter check box and set the new value.

b. To apply the device default value, unselect the Parameter check box.

c. To view the firewall rule default parameters, see Configuring a Default Parameters Map.

d. When you hover your mouse cursor over the Advanced Options icon, the configured parameters are displayed in the quick view window.

Table 50-1 lists the elements on the policy rule page.

Step 12 Click Save to apply the rule to the device. For description of the elements, see the Cisco Prime Infrastructure 3.1 Reference Guide.

Monitoring Policy Rules

The monitoring feature allows you to monitor policy rules. You can identify the most-used rules, and you can troubleshoot a specific rule and verify hits for the selected rule.

To monitor policy rules, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices, then select a device.

Step 2 In the Feature Configuration pane, expand the Security subfolder.

Step 3 In the Security subfolder, expand the Zone Based Firewall and then click Policy Rules. The Firewall Rules page appears.

Step 4 In the Firewall Rules page, click Hit Counters and use one of the following options to analyze the sessions and packets hit counters for the firewall rules.

Step 5 Click the Show all option to view the packets and sessions counters for all firewall rules. The packets and sessions counters are displayed in two separate columns.
Creating a Zone-Based Firewall

Note
When you select the Show all option, the system will display a warning message stating that it may take more time to complete this operation. Sessions hit counters are not applicable for Drop/Pass rules. Similarly, packet hit counters are not applicable for Inspection rules.

Step 6
To know the time of the last update for the rules, hover the mouse cursor over the column names or click the Last Update Time option in the Hit Counters.

Step 7
Click the Show for selected rules option to show the hit counters for a specific rule or a couple of selected rules. The hit counters would be displayed in a popup dialog box with a refresh button that allows quick refresh of the data.

Step 8
Use the predefined filters options available in the top-right corner of the table to display the rules at the top or bottom based on the packets/sessions counts.

Step 9
Click Reset All Counters to discard all of the rules counters on the device. The application will display a warning message before resetting the rules counters.

Editing a Policy Rule

To edit a policy rule, follow these steps:

Step 1
Choose Inventory > Device Management > Network Devices, then select a device.

Step 2
In the Feature Configuration pane, expand the Security subfolder.

Step 3
In the Security subfolder, expand the Zone Based Firewall and then click Policy Rules. The Firewall Rules page appears.

Step 4
In the Firewall Rules page, choose one of the following options:

- Click the Rules parameters row and edit the parameters.
- Select the check box to select the rule, and then click Edit. The selected Rule opens for edit. You cannot edit the name of the policy rule.

Note
You can specify the Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) port range in the firewall rule service. When you add a new rule or edit an existing rule under the Service column, click object selector to assign the TCP / UDP, and click OK. You can define the port numbers in the text box that appears near the protocol icon. Also, you can define the port range in the format of <start-port-number>-<end-port-number>, and this range can be configured for that specific protocol (TCP or UDP).

- You can re-order firewall rules by dragging a rule and dropping it in a different location.

Step 5
Click Save to apply the changes in the device.

Creating a Service Group

You can create, update or delete a service groups. Service group provides an option to group together several port-based applications to logical groups which could be used in firewall policies.
For example, you can define a browsing service-group object and assign both HTTP and HTTPS applications to it. Then you can use this browsing service-group in firewall rules to permit or deny browsing traffic, rather than selecting both HTTP and HTTPS in those rules.

To create a service group, follow these steps:

1. **Step 1** Choose **Inventory > Device Management > Network Devices**, then select a device.
2. **Step 2** In the Feature Configuration pane, expand the **Security** subfolder.
3. **Step 3** In the Security subfolder, expand the **Zone Based Firewall > Common Building Blocks**, and then click **Service Groups**. The Service Groups page appears.
4. **Step 4** To create the Service Group:
   a. In the Service Group page, click **Add Service Group** and enter the Service Group Name. You cannot change the name after creating the Service Group. Also, you cannot create a service group without an application (see **Creating Custom Applications**).
   b. To assign Applications, click the down arrow icon.
   c. In the Applications dialog box, select the **Applications** check box to select one or more applications from the list, then click **OK**.
5. **Step 5** To edit an existing Service Group, do one of the following:
   - In the Service Groups page, click the Service Group parameters row and edit the parameters.
   - Select the service group and click **Edit**. You can add new applications or remove an already selected application.
   - To remove an application from the selected list, hover your mouse cursor over the application name and click **X**.
6. **Step 6** Click **Save** to apply your changes to the device.

### Assigning TCP/UDP Ports on an Application

You can assign or unassign the Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) ports to an application.

**Note**

When you click **Save** in the following procedure, your changes are deployed on the device. You cannot review the requested operation or remove the request from the pending changes queue.

To assign or unassign TCP/UDP ports for an application, follow these steps:

1. **Step 1** Choose **Inventory > Device Management > Network Devices**, then select a device.
2. **Step 2** In the Feature Configuration pane, expand the **Security** subfolder.
3. **Step 3** In the Security subfolder, expand the **Zone Based Firewall > Common Building Blocks**, and then click **Port Mappings**. The Port Application Mapping page appears.

**Note**

Displays the application name that is driven from the device.
Step 4  To assign or unassign the TCP/UDP ports to an application, click the application and update its TCP/UDP ports value. The TCP/UDP Port values are assigned to the specific application.

   a. Assign port(s) by defining one or more ports separated by comma (For example: 1234, 2222 and so on).
   b. Assign port(s) by defining the port range (For example: 1111-1118). You can also assign a combination of ports and port ranges.
   c. Unassign port(s) by deleting the existing port values.

Step 5  Click **Save** to save the configurations.

---

### Configuring a Default Parameters Map

To configure a default parameters, follow these steps:

**Step 1**  Choose **Inventory > Device Management > Network Devices**, then select a device.

**Step 2**  In the Feature Configuration pane, expand the **Security** subfolder.

**Step 3**  In the Security subfolder, expand the **Zone Based Firewall** and then click **Default Parameters**. The Default Parameters page appears.

**Step 4**  In the Default Parameters page, change the parameters value.

**Note**  You can change the default parameters only on ISR devices.

**Step 5**  Click **Save** to save the configuration.

---

### Assigning an Interface for a Zone

The interfaces view gives an overview of the interfaces on the device which are applicable for firewall inspection. The view allows viewing and modifying the assignment of those interfaces to security zones.

To assign or unassign an interface for a zone, follow these steps:

**Step 1**  Choose **Inventory > Device Management > Network Devices**, then select a device.

**Step 2**  In the Feature Configuration pane, expand the **Security** subfolder.

**Step 3**  In the Security subfolder, expand the **Zone Based Firewall** and then click **Interfaces**.

**Step 4**  In the Interface page, select the interface that you want to change and click the down arrow icon. The Zone dialog box appears.

**Step 5**  In the Zone dialog box, select the new security zone for the interface. If the selected interface is already assigned to a zone, you will get a warning message.

**Step 6**  Click **Yes** on the warning message if you want to change the assignment of that interface.

**Step 7**  To un-assign the interface from the specific zone, select the interface and delete the zone information.
Creating a Routing Protocol

A routing protocol specifies how routers:

- Communicate with other routers in a network
- Select routing paths to transmit data between nodes in a computer network
- Share network information with other routers

The following sections describe the routing protocols supported by Prime Infrastructure.

Creating a Static Route

Static routing is the simplest form of routing, where the network administrator manually enters routes into a routing table. The route does not change until the network administrator changes it. Static routing is normally used when there are very few devices to be configured and the administrator is very sure that the routes do not change. The main drawback of static routing is that a change in the network topology or a failure in the external network cannot be handled, because routes that are configured manually must be updated to fix any lost connectivity.

To create a static route, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Choose the device from the list or click Add Device to create a new device, then configure the device.

Step 3 After selecting the device, click Configuration. The Feature Configuration pane appears.

Step 4 Expand the Routing folder, and then click Static. The Static Routing page appears with options to configure IPv4 static routes.

Step 5 To configure an IPv4 static route, do the following:

  a. In the IPv4 Static Routes page, click Add Row, and then complete the fields.
     For Permanent Route, choose either of the following:
     - True to specify that the route will not be removed from the routing table, even if the next-hop interface shuts down or the next-hop IP address is not reachable.
     - False to specify that the route will be removed from the routing table, even if the next-hop interface shuts down or the next-hop IP address is not reachable.

  b. Click Save.

  c. Click Save to save the configuration.
Creating a RIPv2 Route

Routing Information Protocol (RIPv2) is a distance-vector routing protocol that uses hop count as a routing metric. RIPv2 implements a limit of 15 hops in a path from source to a destination, to prevent routing loops. The hop-count limit also limits the size of the networks that RIPv2 supports. RIPv2 sends its routing table every 30 seconds.

The variants of RIPv2 are RIPv2 version 1 (described in RFC1058) and RIPv2 version 2 (described in RFC2453). RIPv2 uses the split horizon, route poisoning, and holddown mechanisms to prevent incorrect routing information from being propagated.

To create a RIPv2 route, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 Choose the device from the list or click Add Device to create a new device, then configure the device.
Step 3 After selecting the device, click Configuration. The Feature Configuration pane appears.
Step 4 Expand the Routing folder, and then click RIPv2. The RIPv2 Routing page appears with options to configure IPv4 RIPv2 routes.
Step 5 To configure an IPv4 RIPv2 route, do the following:
   a. In the IPv4 RIPv2 Routes page, select the RIPv2 version.
   b. Click Add Row, and then complete the fields.
   c. Click Save.
   d. Click Passive Interface to select the passive interface that you want to add.
   e. Click Save to save the configuration.

Creating an EIGRP Route

In EIGRP (an enhanced Interior Gateway Routing Protocol) when an entry in the routing table changes in any of the routers, it notifies its neighbors of the change only, rather than sending the entire routing table. Every router in the network sends a “hello” packet periodically so that all routers on the network understand the states of their neighbors. If a “hello” packet is not received from a router during a certain period of time, it is assumed that the router is inoperative.

EIGRP uses the Diffusing Update Algorithm (DUAL) to determine the most efficient route to a destination and provides a mechanism for fast convergence. Routers using EIGRP and IGRP can interoperate because the routing metric used with one protocol can be easily translated into the routing metric of the other protocol.

To create an EIGRP route, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 Choose the device from the list or click Add Device to create a new device, then configure the device.
Step 3 After selecting the device, click Configuration. The Feature Configuration pane appears.
Step 4 Expand the Routing folder, and then click EIGRP. The EIGRP Routing page appears with options to configure IPv4 EIGRP routes.
Step 5  To configure an IPv4 EIGRP route, do the following:
   a. In the IPv4 EIGRP Routes page, click Add Row, and then complete the fields.
   b. Click Save.
   c. Click Add Interface to select the passive interface that you want to associate to the Autonomous System (AS) number created.
   d. Click Save to save the configuration.

Creating an OSPF Route

Open Shortest Path First (OSPF) is a standards-based routing protocol that uses the Shortest Path First (SPF) algorithm to determine the best route to its destination. OSPF sends Link State Advertisements (LSAs) to all other routers within the same area. OSPF only sends routing updates for the changes only; it does not send the entire routing table.

To create an OSPF route, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 Choose the device from the list or click Add Device to create a new device, then configure the device.
Step 3 After selecting the device, click Configuration. The Feature Configuration pane appears.
Step 4 Expand the Routing folder, and then click OSPF. The OSPF Processes page appears with options to configure IPv4 OSPF processes.
Step 5 To configure an IPv4 OSPF process, do the following:
   a. In the IPv4 OSPF Processes page, click Add Row, and then complete the fields.
   b. Click Save.
   c. Click Passive Interfaces to select the passive interface that you want to associate to the process created.
   d. Click Advanced. The Advanced OSPF IPv4 Configuration dialog box appears.
   e. Click Networks > Add Row, and then complete the fields.
   f. Click Route Summarization > Add Row, and then complete the fields.
   g. Click OK.
   h. Click Save to save the configuration.

Configure QoS for a Device

To enable or disable QoS for a device, follow the below steps.

Step 1 Choose Configuration > Network > Network Devices.
Step 2 Click on the device name for which you want to enable QoS, then select App Visibility & Control > QoS.
Step 3 Select the QoS capable interface and click Enable QoS.
Step 4 Check the Enable QoS on Ingress check box or Enable QoS on Egress check box or both the check boxes depending on your requirement.

Step 5 If you select Enable QoS on Ingress, choose a profile from the Select Profile drop-down list and click OK.

Step 6 If you select Enable QoS on Egress, do the following:
   a. Click the Classify based on profile radio button and choose a profile from the Select Profile drop-down list.
   b. For QoS scheduling, choose a Scheduling action based on profile from the Select Profile drop-down list.

Note You must choose the same profile, if you have chosen both Enable QoS on Ingress and Enable QoS on Egress in Step 4.

Step 7 Click the CLI Preview tab to preview the QoS configuration before deployment.

Step 8 Click Deploy.

Step 9 To disable QoS for a device, do the following:
   a. Click Disable QoS and select on which direction (ingress/egress) to remove QoS configuration from the device.
   b. Click Deploy.

Configuring NAM with Application Servers

Prime Infrastructure supports various features to be configured on NAM, remotely. The NAM Application Servers feature enables you to configure the NAM device with Application servers.

To Configure the parameters of the Application servers, with NAM device, follow these steps:

Step 1 Choose Services > Application Visibility & Control > NAM Application Servers.

Step 2 Click Add.

Step 3 Enter the IP address of the server in Add Servers dialog box and click Add button inside the dialog box. The list of server IP addresses are displayed under IP address column.

Step 4 Select the IP addresses of the servers to be deployed to the NAM device, then Click Add to NAM Server lists.

Step 5 Select the IP Address of one or more of the NAM devices in the Add Server(s) to NAM Server List dialog box, and click Add button within the dialog box. The selected device IP addresses are displayed under Part of NAM Server List on column, and the server parameters get configured on the selected NAM devices.
Ensuring Consistent Application Experiences

Prime Infrastructure can help ensure high-quality WAN end-user experiences across applications at multiple sites.

- Evaluating Service Health
- Establishing Performance Baselines
- Identifying Optimization Candidates
- Validating Optimization ROI
- Monitoring Optimized Flows

Note

To use this feature, your Cisco Prime Infrastructure implementation must include Assurance licenses.

Network operations staff must share a common data resource that gives them complete visibility into network performance data throughout every stage of the optimization cycle, including:

- Identifying the sites and applications that are candidates for optimization, so that network designers can plan where application optimization is critical (see Evaluating Service Health).
- Establishing site and application performance baselines (see Establishing Performance Baselines).

Prime Infrastructure performs baselining for key performance metrics and detects abnormal deviations of baselined values. The key performance metrics include:

- Server Response Time
- Client Transaction Time
- Network Round-Trip Time
- MOS score
- Jitters
- Packet loss
- Bytes sent/received
- Interface utilization
- CPU Utilization
- Memory Utilization
Prime Infrastructure determines the baseline (mean) for each metric by taking the average values of the metric during the last 30 days. Average values are computed separately for each hour of the day for each monitored entity (such as interface, host, site, or application). For example, the baseline for HTTP response time of a given server between 9AM to 10AM today will be different from the baseline of the same server between 7PM to 8PM yesterday.

Prime Infrastructure also computes the metrics’ standard deviations using the last 30 days of data. Similar to averages, standard deviations are computed separately for each hour of the day for each monitored entity.

• Post-implementation validation that WAN performance and application stability have actually improved (see Validating Optimization ROI).

Because the mean and standard deviation of each metric vary over time, Prime Infrastructure continuously reevaluates the thresholds used to compute the health scores (adaptive thresholds). Prime Infrastructure computes baselines and thresholds every hour, and evaluates health scores every five minutes. In each interval:

a. Health scores are computed for every application-site combination.

b. These health scores are aggregated to derive the overall health of each business-critical application (across all sites) and overall health of each site (across all business-critical applications).

When aggregating across sites/applications, the worst scores are used. For example, if any business-critical application of a given site is rated “red,” that site is also rated “red” for that interval. See Health Rules for more information.

• Ongoing monitoring and troubleshooting of the optimized flows (see Monitoring Optimized Flows).

Using the baseline means and standard deviations, Prime Infrastructure can monitor application and service health issues by detecting abnormal deviations of key metrics from their baselined values and assign a health scores (red, yellow, or green) for each application and site for each monitoring interval.

– A red score indicates a highly abnormal deviation from baseline (deviations from baselines with a probability of less than 0.1%).

– A yellow score indicates a mildly abnormal deviation (deviations with a probability of less than 1%).

– A green score indicates that the metric is within its normal range.

– A gray score indicates there is insufficient data for a site/application.

Cisco Prime Infrastructure offers a consistent data resource for each of these stages in performance optimization.

Evaluating Service Health

Choose Services > Application Visibility & Control > Service Health to view the sites and their business critical applications. Each application for a site is given a score for each of the KPIs (Key Performance Indicators) that are available in the system:

• Traffic (megabits per second)

• Client Experience (varies based on application type: average transaction time for transaction-based applications such as HTTP, or MOS code for real-time applications such as RTP)

• Network Performance (average network time for HTTP, jitter and Package Loss for RTP)
• **Application Response** (applicable only for transaction-based applications such as HTTP)

The KPI scores can come from multiple data sources; scores are computed across all data sources for all of the KPIs, and the overall score in the main dashboard is an aggregate of these scores. Scores are assigned as red, yellow, or green based on the warning and critical threshold values assigned in Health rules page. You can navigate to this page by clicking **Launch Health Rules** in the Services > Application Visibility & Control > Service Health page. You can use this option to modify the health rule settings as necessary for your network.

For data to be displayed in Service Health, there must be at least one hour of data. After the first hour, the previous hour’s data is overlaid on the data line as the historical data for the next hour. After the first day, standard deviation and mean are based on the hourly data for the previous day.

These scores are stored for seven days. When you view the data for a previous day, the maximum moving time interval is six hours (you can look at up to six hours of data at a time).

### Creating Custom Applications

Choose **Services > Application Visibility & Control > Applications and Services** to create and manage custom applications and services. Services are groups of applications. Prime Infrastructure provides a default set of applications and services consistent with the Cisco NBAR standard. (See [http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html](http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html) for more information.)

The **All Applications** table shows the list of all predefined and user-defined applications. You can configure some of the applications as **Business Critical applications**.

You can create custom applications that contain the definitions you require and which are not available (either from the device or from Prime Infrastructure). After you create an application, you can deploy the application to the supported devices. Deploying the application definition to the device makes Netflow exported data consistent with Prime Infrastructure and other management tools.

If you deploy a custom application to a device and later want to remove it, you must undeploy the application using the **Applications and Services** option. If you delete the custom application from Prime Infrastructure only, the custom application remains active on the device.

Applications without definitions are displayed as “unknown.”

Custom applications are organized under services; services are organized by category and subcategory to align with the Cisco NBAR standard. For more information about NBAR, see [http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html](http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html).

To create a custom application, follow these steps:

---

**Step 1** Choose **Services > Application Visibility & Control > Applications and Services**.

**Step 2** Click **Create**.

**Step 3** Complete the required **General** and **Attributes** fields.

**Step 4** Choose the traffic classification rule from the **Rule** drop-down list.

**Step 5** Click the **Condition** drop-down list and enter the required values in the applicable fields based on the chosen rule.

**Step 6** Click the Plus icon to add more traffic rules and conditions.

**Step 7** Click **Create**.

The newly created application appears in the **All Applications** table.
Step 8   Choose the newly created application and click **Deploy**.

Step 9   Choose the devices on which you want to deploy this application and click **Submit**.

Step 10  Click **View Jobs** to view the status of the deployment job.

---

**Service Health Window**

The Service Health window allows you to view the information shown in Figure 51-1 and described in Table 51-1.

**Figure 51-1   Services > Application Visibility & Control > Service Health Window**

Table 51-1   Services > Application Visibility & Control > Service Health Window Descriptions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lists the location groups for the filter you selected.</td>
</tr>
<tr>
<td>2</td>
<td>Click to toggle between the Health Summary and the Health Timeline.</td>
</tr>
<tr>
<td>3</td>
<td>Provides quick links to:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Health Rules</strong> page, where you can modify the health rule settings as necessary for your network.</td>
</tr>
<tr>
<td></td>
<td>• View and modify the currently defined business critical applications.</td>
</tr>
<tr>
<td>4</td>
<td>Displays the filter you’re currently viewing. You can click any filter to remove it and refresh the window.</td>
</tr>
<tr>
<td>5</td>
<td>Lists the business critical applications.</td>
</tr>
<tr>
<td>6</td>
<td>Colored symbols indicate good, warning, and critical threshold values based on the health rule setting specified in <strong>Health Rules</strong> page.</td>
</tr>
<tr>
<td>7</td>
<td>Move the slider to specify the time range in which you want to view service health information.</td>
</tr>
</tbody>
</table>
Viewing the Health Timeline

Choose Services > Application Visibility & Control > Service Health, then click Health Summary. Prime Infrastructure changes to display the health information in a timeline.

Health Rules

The data displayed in Services > Application Visibility & Control > Service Health is computed using health rules. You can customize the health rules by clicking the desired row and editing the Critical and Warning values.

- Critical—turns red when the data value exceeds the specified Critical value.
- Warning—turns yellow when the data value exceeds the Warning value.

If the health rule does not exceed the specified Critical or Warning values, it is green.

For example, for Traffic Rate, you might specify the T1 the baseline value of 100 Mbps for a given site, application, and datasource, and the standard deviation value of 20 Mbps.

If the Traffic Rate exceeds 161.8 Mbps, which is 100+(3.09 x 20), you see a red bar indicating a critical warning.

You can click any of the colored bars to get further details.

Enabling Baselining

Standard deviation and mean values are used to compute the scores in Service Health. Baselining is not enabled by default. When baselining is enabled:

- The blue box indicates the standard deviation.
- The blue line indicates the mean value for that hour.
Figure 51-2 Sample Baseline Values

To enable baselining, follow these steps:

**Step 1** Choose Dashboard > Performance > Application.

Baselining is supported by these dashlets:
- Application Traffic Analysis—Shows the aggregate bandwidth rate/volume for a site/enterprise one application, service, or set of applications.
- Application ART Analysis—Shows the response times for a transaction.

**Step 2** To enable application traffic analysis baselining:

a. Open the Application Traffic Analysis dashlet, hover your cursor over the dashlet icons and click Dashlet Options.

b. Select the Baseline check box and save your changes.

**Step 3** To enable application response time analysis baselining:

a. Open the Application ART Analysis dashlet, hover your cursor over the dashlet icons and click Dashlet Options.

b. Choose a metric from the Metric Type drop-down list.

   If you choose the Server Response Time metric, you can select an individual Application Server to see what the response time of that server has been in the past.

c. Select the Baseline check box and save your changes.
Establishing Performance Baselines

Follow these steps to establish the standard performance characteristics of your candidate applications and sites before implementing WAN optimizations.

**Step 1** Choose **Dashboard > Performance > Application**.

**Step 2** Add the following dashlets (see Adding Dashlets) to this page:

- Worst N Clients by ART Metrics
- Worst N Sites by ART Metrics
- Application Server Performance
- Application Traffic Analysis

**Step 3** Use these dashlets to establish the performance characteristics of your optimization candidates as currently configured.

- **Worst N Clients by ART Metrics**: For the worst-performing clients and applications: Maximum and average transaction times, and 24-hour performance trend.
- **Worst N Sites by ART Metrics**: The same information for the worst-performing sites and applications.
- **Application Server Performance**: For all application servers: the maximum and average server response time, and a 24-hour performance trend.
- **Application Traffic Analysis**: Gives 24-hour application traffic metrics in bytes per second and packets per second. Calculates statistical mean, minimum, maximum, median, and first and second standard deviation for the period.

You can sort by any column in any dashlet by clicking the column heading. You can also filter the data in the dashlets by **Time Frame**, **Site**, and **Application**.

**Step 4** Click the **Site** tab and use **Top N Applications**, **Top N Devices with Most Alarms**, **Top N Clients** and **Worst N Clients by ART Metrics** as you did in Step 3.

Identifying Optimization Candidates

Follow these steps to identify your network’s lowest performing applications, clients, servers, and network links.

**Step 1** Choose **Dashboard > Performance > WAN Optimization**.

**Step 2** Add the following dashlets (see Adding Dashlets) to this dashboard.

- Application Traffic
- Server Traffic
- Client Traffic
- Network Links

**Step 3** Using these dashlets, identify the optimization candidates.
Validating Optimization ROI

After you have deployed changes at candidate sites, follow these steps to validate the return on your optimization investment.

Step 1  Choose Dashboard > Performance > WAN Optimization.

The dashlets on this page show:
- **Transaction Time (Client Experience)**—Graphs average client transaction times (in milliseconds) for the past 24 hours, with separate lines for optimized traffic and pass-through traffic (in which optimization is turned off). With optimization enabled, you should see a drop in the optimized traffic time when compared to the pass-through time.
- **Average Concurrent Connections (Optimized vs Passthru)**—Graphs the average number of concurrent client and pass through connections over a specified time period.
- **Traffic Volume and Compression Ratio**—Graphs the bandwidth reduction ratio between the number of bytes before compression and the number of bytes after compression.
- **Multi-Segment Network Time (Client LAN-WAN - Server LAN)**—Graphs the network time between the multiple segments.

Step 2  You can filter the data in the dashlets by Time Frame, Client Site, Server Site, and Application.

Step 3  To generate a report:


b. Specify the filter and other settings for the report, then click Run.
Monitoring Optimized Flows

Follow these steps to monitor optimized WAN traffic.

**Step 1** Choose **Dashboard > Performance > WAN Optimization**.

**Step 2** In the **Multi-Segment Analysis** dashlet, click **View Multi-Segment Analysis**.

**Step 3** Click the **Conversations** tab to see individual client/server sessions, or the **Site to Site** tab to see aggregated site traffic. For each client (or client site) and server (or server site) pair and application in use, these pages show:

- **Average and Max Transaction Time**—The time between the client request and the final response packet from the server. Transaction time will vary with client uses and application types, as well as with network latency. Transaction Time is a key indicator in monitoring client experiences and detecting application performance problems.

- **Average Client Network Time**—The network time between a client and the local switch or router. In Wide Area Application Services (WAAS) monitoring, Client Network Time from a WAE client data source represents the network RTT between the client and its edge WAE, while Client Network Time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).

- **Average WAN Network Time**—The time across the WAN segment (between the edge routers at the client and server locations).

- **Average Server Network Time**—The network time between a server and NAM probing point. In WAAS monitoring, Server Network Time from a server data source represents the network time between the server and its core WAE.

- **Average Server Response Time**—The average time it takes an application server to respond to a request. This is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application server resources, such as the CPU, Memory, Disk, or I/O.

- **Traffic Volume**—The volume of bytes per second in each of the Client, WAN, and Server segments.

**Step 4** Sort and filter the performance data as needed.

- To sort any column, click the column heading.

- You can filter the data displayed by **Time Frame**, or click the Filter icon and specify a Quick or Advanced Filter, or use a Preset Filter.
Troubleshooting Applications

Use the following procedure to determine if there are any problem indications associated with any of the specific applications being run across the network by the end user.

**Before You Begin**
This feature requires:
- Integration with an ISE server (to access endpoint information).
- That session information (NetFlow/NAM data, Assurance licenses) is available.

**Step 1**
To view the applications accessed by the end user and the response time for the applications for the user’s devices, open the User 360° View for that user and click the Applications tab.

**Step 2**
This tab displays the following information:
- Endpoint
- Mac address
- Application
- Last one hour volume (in MB)

To get more information about an application, choose Dashboard > Performance > Application.
Monitoring Microsoft Lync Traffic

You can use Prime Infrastructure to monitor the Microsoft Lync traffic in your network. The Microsoft Lync Software Defined Network (SDN) API provides an interface for network management systems to access Microsoft Lync network diagnostic data for monitoring Lync network traffic and optimizing Microsoft Lync quality of service. Prime Infrastructure processes and filters Microsoft Lync quality update messages and aggregates Microsoft Lync calls. You can view volume trends over time and get a summary of call types, including filtering based on time and location groups. You can also view individual calls and troubleshoot individual call streams.

Note
Prime Infrastructure does not support SDN 2.2 and higher versions.

Related Topics
- Setting Up Lync Monitoring
- Viewing Microsoft Lync Data
- Monitoring End-User Microsoft Lync Experience
- Monitoring Microsoft Lync Data Between Sites

Setting Up Lync Monitoring

You must register Prime Infrastructure as a receiver of Microsoft Lync data in order to monitor and provide a centralized view of how Microsoft Lync is deployed in your network.

On your SDN server, edit the LyncDialogListener.exe file to add the following lines. The LyncDialogListener.exe.config file is located in the Lync SCN API installation directory at the following default location: C:\Program Files\Microsoft Lync Server\Microsoft Lync SDN API.

```xml
<add key="submituri" value="https://PI_server_name/webacs/lyncData"/>
where https://PI_server_name is the name of your Prime Infrastructure as specified in the Trusted Root Certification Authorities certificate.

<add key="clientcertificateid" value="value"/>
where value is the certificate value of your Prime Infrastructure server as specified in the Trusted Root Certification Authorities certificate.

Alternately, if you use the Microsoft SDN interface to enter your Prime Infrastructure server details, you must accept the SSL certificate in order to enable XML communication over secure HTTP.

Text Part Number:
After you register Prime Infrastructure as a receiver of Microsoft Lync data, all Microsoft Lync details are sent to Prime Infrastructure.

**Viewing Microsoft Lync Data**

After you register Prime Infrastructure as a receiver of Microsoft Lync data, all Microsoft Lync details are sent to Prime Infrastructure. To monitor Microsoft Lync data:

**Step 1** Choose Services > Application Visibility & Control > Lync Monitoring.

**Step 2** Click on any of the colored bars, which represent the different call types and the respective call volume over the specified time period, to display additional details. The Lync Conversations table lists the aggregated conversations for the call type you select.

**Step 3** From the Lync Conversations table, click the arrow next to a Caller to expand and view the details of that conversation, from the Caller to the Callee. For example, if you expand a video conversation, there are 4 rows describing the following details:
  - Audio details from Caller to Callee
  - Audio details from Callee to Caller
  - Video details from Caller to Callee
  - Video details from Callee to Caller

**Step 4** Click the Filter icon to view a list of conversations in a selected time frame, from a specific caller site, or from a specific callee site.

**Related Topics**
- Setting Up Lync Monitoring
- Monitoring End-User Microsoft Lync Experience
- Monitoring Microsoft Lync Data Between Sites

**Monitoring End-User Microsoft Lync Experience**

If you receive a call that an end-user is experiencing is having a problem with calls, you can use Prime Infrastructure to view the Microsoft Lync calls for a particular user, and view the list of calls that have the most jitter or packet loss.

**Step 1** Choose Services > Application Visibility & Control > Lync Monitoring.

**Step 2** Click the Filter icon, and then select the site in which the end-user belongs. Prime Infrastructure displays the call volume over the last 6 hours.

**Step 3** If you know the time in which the end-user was experience call problems, click the Filter icon and under Time Filter, enter the parameters for the desired time.

**Step 4** Click on the colored bars that corresponds to Audio call in the time period in which the problems occurred. The Lync Conversations table lists the aggregated conversations for the call type you select.
Step 5

From the Lync Conversations table, click the arrow next to the end-user who experienced call issues to expand and view the details of that conversation, from the Caller to the Callee. For example, if you expand a video conversation, there are 4 rows describing the following details:

- Audio details from Caller to Callee
- Audio details from Callee to Caller
- Video details from Caller to Callee
- Video details from Callee to Caller

Prime Infrastructure displays the call metrics of the conversation.

Related Topics

- Setting Up Lync Monitoring
- Viewing Microsoft Lync Data
- Monitoring Microsoft Lync Data Between Sites

Monitoring Microsoft Lync Data Between Sites

You can use Prime Infrastructure to view the Microsoft Lync data between sites. For example, you can monitor all Microsoft Lync calls that are placed from a particular site to a particular site.

Step 1

Choose Services > Application Visibility & Control > Lync Monitoring.

Step 2

Click the Filter icon, and under Caller Site, select a site from where the Microsoft Lync calls are placed.

Step 3

From the Filter icon, under Callee Site, select a site for where the Microsoft Lync calls are received.

Prime Infrastructure displays the call volume in 5-minute increments for the previous 6 hours for the total calls of each type—video, voice, and appsharing—between the sites you selected.

Understanding Voice Quality Value

When you choose Services > Application Visibility & Control > Lync Monitoring, then click on a call type (audio, video, or application sharing), Prime Infrastructure displays metrics about the Microsoft Lync conversation. Audio call details include a numerical mean opinion score (MOS) value, for which Prime Infrastructure assigns a value that describes the voice quality of the experience that is being delivered to end users as described in the following table:

<table>
<thead>
<tr>
<th>MOS Value</th>
<th>Prime Infrastructure Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater than 3.5</td>
<td>Good</td>
</tr>
<tr>
<td>2-3.5</td>
<td>Fair</td>
</tr>
<tr>
<td>Less than 2</td>
<td>Poor</td>
</tr>
</tbody>
</table>

Related Topics

- Setting Up Lync Monitoring
• Viewing Microsoft Lync Data
• Monitoring End-User Microsoft Lync Experience
Using Mediatrace

Troubleshooting RTP and TCP Flows Using Mediatrace

The Mediatrace troubleshooting tool generates a table that lists the currently active RTP streams or TCP sessions. Using these Mediatrace tables and their associated options, you can:

- Identify and select RTP or TCP flows with problems.
- Troubleshoot problems with RTP or TCP flows.
- Troubleshoot problems with RTP or TCP flows between any two arbitrary endpoints.
- Troubleshoot problems with RTP flows starting from the RTP Conversations dashlet.
- Identify and compare flow performance indicators and data sources.

Related Topics

- Using the Mediatrace Tables
- Running Mediatrace from Selected RTP or TCP Flows
- Launching an Ad Hoc Mediatrace From Endpoints
- Troubleshooting Worst RTP Endpoints Using Dashlets
- Comparing Flow Data From Multiple Sources
- Managing Metrics

Using the Mediatrace Tables

The flow information shown in the RTP Streams and TCP Sessions tables is collected and aggregated from NAM and NetFlow data generated throughout the network.

Many rows in the RTP Streams table are arranged in a tree hierarchy. This will occur whenever an RTP application flow involves more than one data stream. In these cases, the flows between the two application endpoints are aggregated into a single row with a triangle icon.

By default, Prime Infrastructure automatically refreshes the RTP Streams table data every 60 seconds; you can also use one of the preset filters.

Prime Infrastructure refreshes TCP Sessions data once every 300 seconds (5 minutes); you can use the Filter by Application filtering option to include or exclude applications from the list.

You can also click either table’s Refresh button at any time. You can turn off automatic refresh by unselecting the Enable auto refresh check box.
To use the Mediatrace tables:

Step 1  Choose Services > Application Visibility and Control > Mediatrace.
Step 2  From the Application drop-down list, choose RTP or TCP. The page shows the corresponding table: RTP Streams or TCP Sessions.
Step 3  Find the flow that you want to troubleshoot:
- To review all flows with a particular type of issue, click the appropriate column heading to sort on that column.
  For example, if you are monitoring RTP performance across the network and want to see the streams with the worst jitter or packet loss, click the Jitter or Packet Loss column headings to sort the streams on these performance indicators. You can then select any of the streams for troubleshooting.
- To find a particular flow with a problem, click the Quick Filter icon and enter a filter criterion under one or more row headings.
  For example, an end user having trouble accessing an application might report the IP address and the name of that application. You can do a quick filter on the TCP table for either the Client IP address or Application ID, then select that session for troubleshooting.
- To spot issues in RTP subflows, click the triangle icon next to any aggregated RTP flow.
  For example, an RTP voice/video flow between any two endpoints will appear in the RTP Streams table as a single flow with a triangle icon. Clicking the icon will show you the four subflows: an incoming and outgoing video subflow, and an incoming and outgoing voice subflow.
Step 4  To troubleshoot the flow, see the Running Mediatrace from Selected RTP or TCP Flows.

Related Topics
- Running Mediatrace from Selected RTP or TCP Flows
- Using the Mediatrace Tables
- Running Mediatrace from Selected RTP or TCP Flows
- Launching an Ad Hoc Mediatrace From Endpoints
- Troubleshooting Worst RTP Endpoints Using Dashlets
- Comparing Flow Data From Multiple Sources

Running Mediatrace from Selected RTP or TCP Flows

To troubleshoot RTP or TCP flows using Mediatrace:

Step 1  Choose Services > Application Visibility and Control > Mediatrace. In the Application drop-down list, choose RTP or TCP, then find the flow that you want by using the steps in Using the Mediatrace Tables.
Step 2  Select the flow and click Trace Service Path. Prime Infrastructure displays the RTP or TCP Stream Details page for the selected flow, with all of the routers in the flow’s path in the Troubleshooting Status table, in the order of their distance from the flow’s source endpoint. Routers that are Medianet-capable are indicated by a filmstrip icon.
Step 3  
To run Mediatrace or Traceroute from a router in the flow’s path, click the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

The **Start Mediatrace** link is present when the device is Mediatrace-capable; the **Start Traceroute** link is present when the device is not Mediatrace-capable.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where non-Medianet-capable routers were encountered and how they were processed.
- Medianet-capable routers on which Medianet is not configured.

Step 4  
When the operation is complete, the Troubleshooting tab displays a topology map of all of the devices between the flow’s two endpoints. Device icons in the map consist of:

- **Alarm Severity**—The most severe alarm currently recorded for the device.
- **Flag**—The device on which the Mediatrace or Traceroute was initiated.
- **Filmstrip**—The device is Medianet-capable.
- **Minus sign on red background**—The device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder as explained in **Troubleshooting RTP and TCP Flows Using Mediatrace**.
- **Minus sign**—The device is unmanaged.

Step 5  
To see key performance metrics, such as CPU and memory utilization, jitter, and packet loss, for all Medianet-capable devices in the RTP or TCP flow’s path, click the **Medianet Path View** tab. To see the performance metrics in numerical and graphic form, click the subtabs in the Medianet Path View pane.

**Note**  
The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 6  
Use the appropriate links in the Troubleshooting Status table to:

- Launch a Mediatrace or Traceroute operation on a different router.
- Restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

**Related Topics**

- Using the Mediatrace Tables
- Running Mediatrace from Selected RTP or TCP Flows
- Launching an Ad Hoc Mediatrace From Endpoints
- Troubleshooting Worst RTP Endpoints Using Dashlets
- Comparing Flow Data From Multiple Sources
Launching an Ad Hoc Mediatrace From Endpoints

You can quickly launch a Mediatrace against all RTP or TCP flows between any two endpoints in the network. This can include either specific flows running between any two endpoints on the same or different sites, or between a pair of routers on two different sites.

This is handy if your network lacks NAM monitoring, or when you are in a hurry and you know at least the IP addresses of the two endpoints of the RTP or TCP flow. You must still navigate to and start the trace from the appropriate RTP or TCP Mediatrace table.

To launch an ad hoc Mediatrace from two endpoints:

---

**Step 1** Choose **Services > Application Visibility and Control > Mediatrace**. From the **Application** drop-down list, choose **RTP** or **TCP**.

**Step 2** Click **Specify Session for Mediatrace**.

**Step 3** Enter the required information:
- For an RTP flow:
  - Select the **Source Site**.
  - Enter the **Source Endpoint IP address**.
  - Enter the **Destination EndPoint IP address**.
- For a TCP flow:
  - Select the **Client Site**.
  - Enter the **Client Endpoint IP address**.
  - Enter the **Server Endpoint IP address**.

**Step 4** Provide any additional endpoint information that you have:
- For an RTP flow, select or enter the **Source Endpoint Port** and **Destination Endpoint Port**.
- For a TCP flow, select or enter the **Server Endpoint Port**.

**Step 5** Click **Trace Service Path** (for an RTP flow) or **OK** (for a TCP flow). Prime Infrastructure displays the RTP or TCP Stream Details page for the specified flow, with all of the routers in the flow’s path in the Troubleshooting Status table, in the order of their distance from the flow’s source or client endpoint. Routers with a “filmstrip” icon next to them are Medianet-capable.

**Step 6** To run Mediatrace or Traceroute from a router in the flow’s path, click the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:
- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where and how non-Medianet-capable routers where encountered and processed.
- Medianet-capable routers on which Medianet is not configured.

**Step 7** When the operation is complete, the Troubleshooting tab displays a topology map of all the devices between the flow’s two endpoints. Device icons in the map will be badged as follows:
- **Alarm Severity**—The most severe alarm currently recorded for the device.
- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign on red background—The device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder.
- Minus sign—The device is unmanaged.

**Step 8**
To see key performance metrics for all Medianet-capable devices in the flow’s path, click the **Medianet Path View** tab. Click the subtabs in the Medianet Path View pane to see the performance metrics in numerical and graphic form.

**Note**
The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

**Step 9**
Use the appropriate links in the Troubleshooting Status table to launch a Mediatrace or Traceroute operation on a different router, restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

---

**Troubleshooting Worst RTP Endpoints Using Dashlets**

You can quickly launch a Mediatrace against the poorest performing RTP flows in your network using the **Worst N RTP End Point Pairs** and **RTP Conversation** dashlets. This works only for RTP flows.

The **RTP Conversations** dashlet shows the complete history for a source endpoint, including flows that are no longer active. You will want to select only the most recent flows. If you launch Mediatrace on such an inactive flow, you will receive an error message advising you of this fact.

**Step 1**
Choose **Dashboard > Performance > End User Experience**.

**Step 2**
In the **Worst N RTP End Point Pairs** dashlet (if this dashlet is not already in the dashboard, see **Adding Dashlets**), note the Source Address for your worst performing RTP flows.

**Step 3**
In the **RTP Conversations** dashlet in the same page, find the most recent conversation for the same Source Address.

**Step 4**
Select that conversation in the **RTP Conversations** dashlet, then choose **Troubleshoot > Trace Service** path. Prime Infrastructure displays the RTP Stream Details page for the selected flow, with all of the routers in the flow’s path in the Troubleshooting Status table, in order of their distance from the flow’s source endpoint. Routers that are Medianet-capable are indicated by a filmstrip icon.

**Step 5**
To run Mediatrace or Traceroute from a router in the flow’s path, click the **Start Mediatrace** or **Start Traceroute** link next to that router in the table.

**Note**
The **Start Mediatrace** link is present when the device is Mediatrace-capable; the **Start Traceroute** link is present when the device is not Mediatrace-capable.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.
While running Mediatrace or Traceroute, click the **Logs** tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where and how non-Medianet-capable routers were encountered and processed.
- Medianet-capable routers on which Medianet is not configured.

**Step 6**

When the operation is complete, the Troubleshooting tab displays a topology map of all of the devices between the flow’s two endpoints. Device icons in the map will be badged as follows:

- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign—The device is unmanaged.

**Step 7**

To see key performance metrics for all Medianet-capable devices in the flow’s path, click the **Medianet Path View** tab. To see the performance metrics in numerical and graphic form, click the subtabs in the Medianet Path View pane.

**Note**

The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

**Step 8**

Use the appropriate links in the Troubleshooting Status table to:

- Launch a Mediatrace or Traceroute operation on a different router.
- Restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

---

**Comparing Flow Data From Multiple Sources**

When interpreting Mediatrace performance data, you might find it helpful to:

- Identify the NAM, NetFlow, and other sources reporting this performance data.
- If you have multiple NAM or NetFlow data sources, compare how those sources are reporting key performance indicators for a particular flow.

To compare flow data from multiple sources:

**Step 1**

Choose **Services > Application Visibility and Control > Mediatrace**.

**Step 2**

From the **Application** drop-down list, choose **RTP** or **TCP**, then find the flow that you want using the steps in **Using the Mediatrace Tables**.

**Step 3**

Expand a row (for an RTP or TCP flow) to view the details of the key performance indicators appropriate for the selected flow and the data source for each such set of indicators.

**Step 4**

When you are finished, click **OK**.
Cisco Mobility Services Engine and Services

The Cisco Mobility Services Engine (MSE) supports various services within the overall Cisco Unified Wireless Network (CUWN).

The Cisco MSE currently supports the following services:

- **Location Service**—Also known as Context Aware Service (CAS). This is the core service of the MSE that turns on Wi-Fi client tracking and location API functionality. Allows MSE to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as presence, location, telemetry data, and historical information.

- **Wireless Intrusion Protection Service**—Provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption within the CUWN infrastructure. wIPS visualizes, analyzes, and identifies wireless threats, and centrally manages mitigation and resolution of security and performance issues using Cisco monitor mode and Enhanced Local Mode (ELM) Access Points. Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks.

- **Mobile Concierge**—Mobile Concierge enables the Cisco Mobility Services Advertisement Protocol (MSAP). This protocol enables direct communication between the MSE and mobile devices, allowing content to be pushed directly to the mobile device pre-association. This functionality is dependent on the mobile device supporting 802.11u and MSAP.

- **CMX Analytics Service**—The CMX Analytics service analyzes wireless device location information in a particular network. The CMX Analytics service uses the data provided by the MSE to calculate the location of Wi-Fi devices in the Wireless Local Area Network (WLAN). In addition, the FastLocate feature sends information about the RSSI strength of data packets to the Cisco WLC that can be used for location calculations.

When a wireless device is enabled in a network, it transmits probe request packets to identify the wireless network in its neighborhood. Even after connecting to the access point in the WLAN, the client devices continue to transmit probe request packets to identify other access points for better quality of service. The access points gather these request and the associated RSSI from the various wireless devices and forwards them to the Wireless LAN Controller (WLC). The controller then forwards this information to the MSE.

The basic data that is collected from various APs, when analyzed, produces information and knowledge about the movement and behavior patterns of people who are using Wi-Fi devices in the building. For example, the building can be an airport, shopping mall, city center, and so on. The CMX Analytics service helps the airport authorities or the building owners to understand the movement of passengers or customer within their building. This helps them improve the signage, make changes to the under utilized areas, and so on.
Adding MSEs to Prime Infrastructure

You can add an MSE using the Add Mobility Services Engine dialog box in the Mobility Service page. In this dialog box, you can add licensing files, tracking parameters, and assign maps to the MSE. If you launch the wizard with an existing MSE for configuration, then the Add MSE option appears as Edit MSE Details.

Before You Begin

- To learn more about Cisco Adaptive wIPS features and functionality, go to Cisco.com to watch a multimedia presentation. Here you can find the learning modules for a variety of Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.
- The Services > Mobility Services > Mobility Services Engines page is available only in root virtual domain.

To add an MSE to Prime Infrastructure, log in to Prime Infrastructure and follow these steps:

Step 1 Verify that you can ping the mobility service engine that you want to add from Prime Infrastructure.

Step 2 Choose Services > Mobility Services > Mobility Services Engines to display the Mobility Services page.

Step 3 From the Select a command drop-down list, choose Add Mobility Services Engine, and click Go. The Add Mobility Services Engine page appears.

Step 4 Enter the following information:
- Device Name—User-assigned name for the MSE.
- IP Address—The IP address of the mobility service engine.

An MSE is added only if a valid IP address is entered. The Device Name helps you distinguish between devices if you have multiple Prime Infrastructures with multiple mobility services engines, but it is not considered when validating an MSE.

- Contact Name (optional)—The mobility service engine administrator.
- Username—The default username is admin. This is the Prime Infrastructure communication username configured for MSE.
- Password—The default password is admin. This is the Prime Infrastructure communication password configured for MSE.
If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, we recommend that you rerun the automatic installation script and change the username and password.

- Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the MSE.

  This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.

**Step 5** Click **Next**. Prime Infrastructure automatically synchronizes the selected elements with the MSE.

After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license.

**Configuring Services for MSE**

**Step 6** To enable a service on the MSE, select the check box next to the service. The different type of services are:

- **Context Aware Service**—If you select the Context Aware Service check box, then you must select a location engine to perform location calculation. You can choose CAS to track clients, rogues, interferers, and tags. You can choose Cisco Context-Aware Engine for Clients and Tag to track tags.

- **WIPS**—The Wireless Intrusion Prevention System check box, it detects wireless and performance threats.

- **Mobile Concierge Service**—The Mobile Concierge Service check box, it provides service advertisements that describe the available services for the mobile devices.

- **CMX Analytics Service**—The CMX Analytics Service check box, it provides a set of data analytic tools packaged for analyzing Wi-Fi device location data that comes from the MSE.

- **CMX Connect & Engage**—The CMX Connect and Engage service provides a guest Wi-Fi onboarding solution, as well as zone and message configuration for the CMX Software Development Kit (SDK).

- **HTTP Proxy Service**—The HTTP Proxy service on the MSE terminates all HTTP traffic intercepted using Policy Based Routing (PBR) and acts as a forward proxy by pulling contents on behalf of wireless clients.

From release 7.5 onward, wIPS service requires a dedicated MSE because it does not support CAS and wIPS on the same MSE.

**Configuring MSE Tracking and History Parameters**

**Step 7** After you enable services on the MSE, the Select Tracking & History Parameters page appears.

If you skip configuring the tracking parameters, the default values are selected.

**Step 8** You can select the clients that you want to keep track of by selecting the corresponding Tracking check box(es). The various tracking parameters are as follows:

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
Step 9 You can enable the history tracking of devices by selecting the corresponding devices check box(es). The different history parameters are as follows:
- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

Step 10 Click Next to Assign Maps to the MSE.

Assigning Maps to the MSE
The Assigning Maps page is available only if you select CAS as one of the services to be enabled on the MSE.

Step 11 Once you configure MSE tracking and history parameters, the Assigning Maps page appears.
The Assign Maps page shows the following information:
- Name
- Type (building, floor, campus)
- Status

Step 12 You can see the required map type by selecting either All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available on the page.

Step 13 To synchronize a map, select the Name check box, and click Synchronize.
Upon synchronization of the network designs, the appropriate controllers that have APs assigned on a particular network design are synchronized with the MSE automatically.

Step 14 Click Next to configure mobile app enablement.

Mobile App Enablement
Enabling this integration will allow the MSE to send floor maps and wireless client position notification to Meridian. Meridian used this information to provide location-based services to your users without requiring them to connect to your network and access the MSE directly. After enabling Meridian, you will receive an e-mail with instructions on how to activate your account and share access with others in your organization. You can utilize Meridians platform to provide location services to your visitors either through the Meridian mobile app or your own apps using their mobile SDKs for Android and iOS. The data bandwidth for each wireless client position or zone notification from MSE to Meridian can be maximum of 1 MB/second. For more information, please visit http://www.meridianapps.com/mse

Step 15 Once you assign maps to the MSE, the Mobile App Enablement page appears.

Step 16 Select the Enable Mobile App Integration check box to enable the mobile application integration. You can click an icon to open the Mobile App Enablement Help page.

Step 17 Enter the name for the location on the Location Name text box. The name you enter here will appear in the Meridian app so that you can try out the location services on your own device.
Step 18 Enter the email address in the E-mail Address text box to access the Meridian online editor and SDK. Meridian will email these addresses with instructions on how to access your account and share it with others in your organization.

Step 19 Enter the server where the MSE can register its UDI and send the maps that are synchronized to the MSE in the Registration Endpoint text box.

Step 20 Enter the server detail where the MSE can send location update notifications in the data format specified in the Notifications Endpoint text box.

Step 21 Select the Notifications Data Format radio button. This is the data format of the notifications sent from the MSE. The different data formats are: Legacy SOAP/XML, XML, JSON, and Protocol Buffers.

Step 22 Enter the street address of your location in the Street Address text box.

Step 23 Enter the phone number where Meridian can reach you for additional information in the Phone Number text box.

Step 24 Click Advanced to open the Advanced pane.

Step 25 If you want MSE to send real-time notifications to Meridian when ever the wireless clients enter the selected zones, then select the Enable Zone Notifications for zones check box and choose floors and zones from the drop-down list.

The Enable zone notifications for zones drop-down list shows all the floors and zones that are added to Prime Infrastructure and synced to the MSE.

Step 26 Click OK after selecting zones and floors.

Step 27 Click Save.

Step 28 Click Done to save the MSE settings.

Related Topics
- Viewing MSEs
- Deleting MSE License Files
- Deleting MSEs from Prime Infrastructure
- Adding a Location Server

MSE Licensing

The Cisco MSE provides a wide variety of location-based services. To enable these services, the following are required:

- Cisco MSE hardware or software appliance
  - Physical Appliance—An activation license is not required.
  - Virtual Appliance—Virtual Appliance instance requires an MSE Virtual Appliance Activation license (L-MSE-7.0-K9). It is not sufficient to simply have a service/feature license on an MSE Virtual Appliance.
- Licenses
- Support

There are three types of MSE licenses available:
## MSE Licensing

### MSE License Types

<table>
<thead>
<tr>
<th>MSE Service License</th>
<th>Provides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Location License</td>
<td>Advanced spectrum capability with the ability to detect, track, and trace rogue devices, Cisco CleanAir® interferers, Wi-Fi clients, and RFID tags. The Base Location license also enables customers and partners to use standard MSE APIs.</td>
</tr>
</tbody>
</table>
| CMX License               | The Base Location license capabilities plus the CMX features:  
  • CMX Analytics, a user-friendly location analytics platform to view and analyze how, where, and when visitors move through a venue.  
  • CMX Connect and Engage for a customizable and location-aware captive portal to on-board guest users to Wi-Fi including:  
  • CMX for Facebook Wi-Fi, helping guests connect to Wi-Fi and use the Internet. Enterprises or merchants gain social demographic data via Facebook Insights.  
  • CMX SDK for enabling organizations to integrate Wi-Fi-based indoor navigation with push notification and auto-launch capabilities into mobile applications. |
| wIPS License              | Complete wireless threat detection and mitigation in the wireless network infrastructure:  
  • Rogue Detection, Classification, and Mitigation  
  • Over-the-Air Attack Detection  
  • Security Vulnerability Monitoring  
  • Performance Monitoring, and Auto-Optimization  
  • Management, Monitoring, and Reporting  
  Requires a separate MSE running the wIPS service.  
  There are 3 deployment options:  
  • Enhanced Local mode: Number of wIPS licenses required equals the number of access points in local mode (data serving) deployed in the network.  
  • Monitor mode: Number of wIPS licenses required equals the number of access points configured in the full-time monitor mode.  
  • Wireless Security Module (WSM)/Monitor module: Number of wIPS licenses required equals the number of wireless security and spectrum intelligence modules deployed in the network. |

For complete details on ordering and downloading licenses, see the *Cisco Mobility Services Engine Licensing and Ordering Guide* at the following URL:  

### Installing Device and wIPS License Files

You can install device and wIPS licenses from Prime Infrastructure.

**Step 1** Choose Administration > Licenses and Software Updates > Licenses.  
**Step 2** Choose Files > MSE Files.  
**Step 3** Click Add. The Add a License File dialog appears.  
**Step 4** Choose the appropriate MSE name from the MSE Name drop-down list.
Step 5  Verify that the UDI of the selected MSE matches the one you entered when registering the PAK.

Step 6  Click **Choose File** to browse and to select the license file.

Step 7  Click **Upload**. The newly added license appears in the MSE license file list.

---

**Viewing MSE License Information**

The license center allows you to manage Prime Infrastructure, Wireless LAN Controllers, and MSE licenses. To view the license information, follow these steps:

**Step 1**  Choose **Administration > Licenses and Software Updates > Licenses**.

**Step 2**  Choose **Summary > MSE** from the left sidebar menu, to view the summary page.

The MSE Summary page displays the following information. See Table 55-2.

---

**Table 55-2: General Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE Name</td>
<td>Provides a link to the MSE license file list page.</td>
</tr>
<tr>
<td>Service</td>
<td>Type of service using: CAS or wIPS.</td>
</tr>
<tr>
<td>Platform Limit by AP</td>
<td>Platform limit.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of MSE.</td>
</tr>
<tr>
<td>Installed Limit by AP</td>
<td>Displays the total number of client elements licensed across MSEs.</td>
</tr>
<tr>
<td>License Type</td>
<td>The three different types of licenses. They are permanent, evaluation, and extension.</td>
</tr>
<tr>
<td>Count by elements</td>
<td>The number of CAS or wIPS elements currently licensed across MSEs.</td>
</tr>
<tr>
<td>Unlicensed Count</td>
<td>Displays the number of client elements that are not licensed.</td>
</tr>
<tr>
<td>%Used</td>
<td>The percentage of CAS or wIPS elements licensed across MSEs.</td>
</tr>
</tbody>
</table>

---

**Deleting MSE License Files**

To delete an MSE license file, follow these steps:

**Step 1**  Choose **Services > Mobility Services > Mobility Service Engine**.

The Mobility Services page appears.

**Step 2**  Click **Device Name** to delete a license file for a particular service.

**Step 3**  From the Select a command drop-down list, choose **Edit Configuration**.

**Step 4**  Click **Next** in the Edit Mobility Services Engine dialog box.

The MSE License Summary page appears.

**Step 5**  Choose the MSE license file that you want to delete in the MSE License Summary page.
### Viewing MSEs

To see a list of current Mobility Services, choose **Services > Mobility Services > Mobility Services Engines**.

The Mobility Services Engines page provides device information and features for each device and a Select a command drop-down list.

Location and MSE features of Prime Infrastructure do not support partitioning.

**Related Topics**
- Viewing MSEs
- Adding MSEs to Prime Infrastructure
- Deleting MSE License Files
- Deleting MSEs from Prime Infrastructure
- Synchronizing Prime Infrastructure and MSE

### Deleting MSEs from Prime Infrastructure

To delete an MSE from the Prime Infrastructure database, follow these steps:

1. **Step 1**
   - Choose **Services > Mobility Services > Mobility Services Engines**.
   - The Mobility Services page appears.

2. **Step 2**
   - Select the MSE(s) to be deleted by selecting the corresponding **Device Name** check box(es).

3. **Step 3**
   - From the Select a command drop-down list, choose **Delete Service(s)**.

4. **Step 4**
   - Click **Go**.

5. **Step 5**
   - Click **OK** to confirm that you want to delete the selected MSE from the Prime Infrastructure database.

6. **Step 6**
   - Click **Cancel** to stop the deletion.
Adding a Location Server

To add a location server, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** From the Select a command drop-down list, choose Add Location Server.

**Step 3** Click Go.

**Step 4** Enter the required information:

**Step 5** Select the Delete synchronized service assignments check box if you want to permanently remove all service assignments from the MSE.

This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.

**Step 6** Click Save.

After adding a location server, it must be synchronized with Prime Infrastructure. See the Synchronizing Prime Infrastructure and MSE for more information.

Location and MSE features of Prime Infrastructure do not support partitioning.

Related Topics

- Viewing MSEs
- Adding MSEs to Prime Infrastructure
- Deleting MSEs from Prime Infrastructure

Synchronizing Prime Infrastructure and MSE

This section describes how to synchronize Prime Infrastructure and MSEs manually and smartly.

After adding an MSE to Prime Infrastructure, you can synchronize network designs (campus, building, floor, and outdoor maps), controllers (name and IP address), specific Catalyst 3000 Series and 4000 switches, and event groups with the MSE.

- Network Designs—A logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus and the floors of each building constitute a single network design.
- Controllers—A selected controller that is associated and regularly exchanges location information with an MSE. Regular synchronization ensures location accuracy.
- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked.
Wired Switches — Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.

- The MSE can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.

- The MSE can also be synchronized with the following Catalyst series switches 4000: WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE

Third Party Elements — When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

Service Advertisements — Mobile Concierge Service provides service advertisements on the mobile devices. This shows the service advertisement that has synchronized with the MSE. Be sure to verify software compatibility between the controller, Prime Infrastructure, and the MSE before synchronizing.

Communication between the MSE, Prime Infrastructure, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with the UTC time. The MSE and its associated controllers must be mapped to the same NTP server and the same Prime Infrastructure server. An NTP server is required to automatically synchronize time between the controller, Prime Infrastructure, and the MSE.

Related Topics
- Viewing MSEs
- Synchronizing Prime Infrastructure Network Designs, Controllers, Wired Switches, or Event Groups
- Synchronizing Controllers with MSEs
- Managing Third-Party Elements on MSEs
- Configuring Smart Mobility Services Engine Database Synchronization
- Viewing Synchronization History

Synchronizing Prime Infrastructure Network Designs, Controllers, Wired Switches, or Event Groups

To synchronize Prime Infrastructure network designs, controllers, wired switches, or event groups with the MSE, follow these steps:

**Step 1** Choose **Services > Mobility Services > Synchronize Services**.

**Step 2** Choose the appropriate menu option (Network Designs, Controllers, Event Groups, Wired Switches, Third Party Elements, or Service Advertisements) from the left sidebar menu.

**Step 3** To assign a network design to an MSE, from the left sidebar menu, choose **Network Designs**.

**Step 4** Select all the maps to be synchronized with the MSE by selecting the corresponding **Name** check box. Through 6.0, you can assign only up to a campus level to an MSE. Beginning with 7.0 this option is granular to a floor level. For example, you can choose to assign floor1 to MSE 1, floor2 to MSE 2, and floor3 to MSE 3.

**Step 5** Click **Change MSE Assignment**.
Step 6 Select the MSE to which the maps are to be synchronized.
A network design might include a floor in a campus or a large campus with several buildings, each monitored by a different MSE. Because of this, you might need to assign a single network design to multiple MSEs.

Step 7 Click either of the following in the MSE Assignment dialog box:

- **Save**—Saves the MSE assignment. The following message appears in the Messages column of the Network Designs page with a yellow arrow icon:
  “To be assigned - Please synchronize”.

- **Cancel**—Discards the changes to the MSE assignment and return to the Network Designs page.

You can also click **Reset** to undo the MSE assignments.

A network design may include a floor in a campus or a large campus with several buildings, each monitored by a different MSE. Because of this, you may need to assign a single network design to multiple MSEs.

Network design assignments also automatically picks up the corresponding controller for synchronization.

Step 8 Click **Synchronize** to update the MSE(s) database(s).
When items are synchronized, a green two-arrow icon appears in the Sync.
You can use the same procedure to assign wired switches or event groups to an MSE.

**Related Topics**

- Synchronizing Prime Infrastructure and MSE
- Viewing Synchronization History
- Synchronizing Controllers with MSEs
- Configuring Smart Mobility Services Engine Database Synchronization, page 55-xiv
- Out-of-Sync Alarms

**Synchronizing Controllers with MSEs**

You can assign an MSE to any wireless controller on a per-service (CAS or wIPS) basis.
To assign an MSE service to wireless controllers, follow these steps:

**Step 1** In the synchronization page, choose **Controllers**.

**Step 2** Choose the controllers to be assigned to the MSE.

**Step 3** Click **Change MSE Assignment**.

**Step 4** Choose the MSE to which the controllers must be synchronized.

**Step 5** Click either of the following in the dialog box:

- **Save**—Saves the MSE assignment. The following message appears in the Messages column of the Controllers page:
  “To be assigned - Please synchronize”.

- **Cancel**—Discards the changes to the MSE assignment and returns to the Controllers page.
You can also click **Reset** to undo the yellow button assignments.

**Step 6**  
Click **Synchronize** to complete the synchronization process.

**Step 7**  
Verify that the MSE is communicating with each of the controllers for only the chosen service. This can be done by clicking the **NMSP status** link in the status page. See **Troubleshooting NMSP Status** for more information.

After Synchronizing a controller, verify that the timezone is set on the associated controller. Controller names must be unique for synchronizing with an MSE. If you have two controllers with the same name, only one is synchronized.

To unassign a network design, controller, wired switch, or event group from an MSE, follow these steps:

**Step 1**  
On the respective tabs, click one or more elements, and click **Change MSE Assignment**. The Choose MSE dialog box appears.

**Step 2**  
Unselect the **Mobility Services Engine** check box if you do not want the elements to be associated with that MSE.

**Step 3**  
Click **Save** to save the changes to the assignments.

**Step 4**  
Click **Synchronize**. A two-arrow icon appears in the Sync Status column.

**Related Topics**

- **Troubleshooting NMSP Status**
- **Viewing MSEs**
- **Synchronizing Prime Infrastructure and MSE**
- **Viewing Synchronization History**
- **Synchronizing Prime Infrastructure and MSE**
- **Configuring Smart Mobility Services Engine Database Synchronization**

**Troubleshooting NMSP Status**

If you recently upgraded a controller and NMSP status is inactive on the **Services > Mobility Services > Synchronize Services > Controllers** page, you need to trigger an inventory collection so Prime Infrastructure receives the upgraded controller information:

**Step 1**  
Choose **Administration > Dashboards > Job Dashboard**.

**Step 2**  
Select **System Jobs > Inventory**, then select **Wireless Controller Inventory**.

**Step 3**  
Click **Run**.

After the job completes, the NMSP Status will be updated.
Managing Third-Party Elements on MSEs

When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

To delete the elements or mark them as third-party elements, follow these steps:

**Step 1**
Choose Services > Mobility Services > Synchronize Services.

The Network Design page appears.

In the Network Design page, choose Third Party Elements from the left sidebar menu.

The Third Party Elements page appears.

**Step 2**
Select one or more elements.

**Step 3**
Click one of the following buttons:

- **Delete Event Groups**—Deletes the selected event groups.
- **Mark as 3rd Party Event Group(s)**—Marks the selected event groups as third-party event groups.

**Related Topics**

- Viewing MSEs
- Synchronizing Prime Infrastructure and MSE
- Viewing Synchronization History
- Synchronizing Prime Infrastructure and MSE
- Configuring Smart Mobility Services Engine Database Synchronization
- Synchronizing Controllers with MSEs
- Out-of-Sync Alarms

Setting and Verifying the Controller Time Zones

For controller Releases 4.2 and later, if an MSE (Release 5.1 or greater) is installed in your network, it is mandatory that the time zone be set on the controller to ensure proper synchronization between the two systems.

Greenwich Mean Time (GMT) is used as the standard for setting the time zone system time of the controller.

You can automatically set the time zone during initial system setup of the controller or manually set it on a controller already installed in your network.

To manually set the time and time zone on an existing controller in your network using the CLI, follow these steps:

**Step 1**
Configure the current local time in GMT on the controller by entering the following commands:

```
(Cisco Controller) >config time manual 09/07/07 16:00:00
(Cisco Controller) >config end
```
When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8 AM Pacific Standard Time (PST) in the US, you enter 16:00 (4 PM PST) as the PST time zone is 8 hours behind GMT.

### Step 2
Verify that the current local time is set in terms of GMT by entering the following command:

```
(Cisco Controller) > show time
Time: Fri Sep 7 16:00:02 2007
Timezone delta: 0:0
```

### Step 3
Set the local time zone for the system by entering the following commands:

When setting the time zone, you enter the time difference of the local current time zone with respect to GMT (+/-). For example, Pacific Standard Time (PST) in the United States (US) is 8 hours behind GMT (UTC) time. Therefore, it is entered as -8.

```
(Cisco Controller) > config time timezone -8
(Cisco Controller) > config end
```

### Step 4
Verify that the controller shows the current local time with respect to the local time zone rather than in GMT by entering the following command:

```
(Cisco Controller) > show time
Time: Fri Sep 7 08:00:26 2007
Timezone delta: -8:0
```

The time zone delta parameter in the `show time` command shows the difference in time between the local time zone and GMT (8 hours). Before configuration, the parameter setting is 0:0.

---

**Related Topics**
- Viewing MSEs
- Synchronizing Prime Infrastructure and MSE
- Viewing Synchronization History
- Synchronizing Prime Infrastructure and MSE
- Synchronizing Controllers with MSEs
- Configuring Smart Mobility Services Engine Database Synchronization
- Managing Third-Party Elements on MSEs

---

**Configuring Smart Mobility Services Engine Database Synchronization**

Manual synchronization of Prime Infrastructure and MSE databases provides immediate synchronization. However, future deployment changes (such as making changes to maps and access point positions), can yield incorrect location calculations and asset tracking until resynchronization reoccurs.

To prevent out-of-sync conditions, use Prime Infrastructure to carry out synchronization. This policy ensures that synchronization between Prime Infrastructure and MSE databases is triggered periodically and any related alarms are cleared.

Any change to one or more of any synchronized components is automatically synchronized with the MSE. For example, if a floor with access points is synchronized with a particular MSE and then one access point is moved to a new location on the same floor or another floor which is also synchronized with the MSE, then the changed location of the access point is automatically communicated.
To further ensure that Prime Infrastructure and MSE are in sync, smart synchronization happens in the background.

To configure smart synchronization, follow these steps:

**Step 1** Choose **Administration > Settings > Background Tasks.**

The Background Tasks summary page appears.

**Step 2** Select the **Mobility Service Synchronization** check box.

**Step 3** The Mobility Services Synchronization page appears.

**Step 4** To set the MSE to send out-of-sync alerts, select the **Enabled** check box in the Out of Sync Alerts group box.

**Step 5** To enable smart synchronization, select the Smart Synchronization **Enabled** check box.

Smart synchronization does not apply to elements (network designs, controllers, or event groups) that have not yet been assigned to an MSE. However, out-of-sync alarms are still generated for these unassigned elements. For smart synchronization to apply to these elements, you need to manually assign them to an MSE.

When an MSE is added to Prime Infrastructure, the data in Prime Infrastructure is always treated as the primary copy that is synchronized with the MSE. All synchronized network designs, controllers, event groups and wired switches that are present in the MSE and not in Prime Infrastructure are removed automatically from MSE.

**Step 6** Enter the time interval, in minutes, that the smart synchronization is to be performed.

By default, smart-sync is disabled.

**Step 7** Click **Submit.**

### Smart Controller Assignment and Selection Scenarios

**Scenario 1**

If a floor having at least one access point from a controller is chosen to be synchronized with the MSE from the Network Designs section of the Synchronization page, then the controller to which that access point is connected is automatically selected to be assigned to the MSE for CAS service.

**Scenario 2**

When at least one access point from a controller is placed on a floor that is synchronized with MSE, the controller to which the access point is connected is automatically assigned to the same MSE for CAS service.

**Scenario 3**

An access point is added to a floor and is assigned to an MSE. If that access point is moved from controller A to controller B, then controller B is automatically synchronized to the MSE.

**Scenario 4**

If all access points placed on a floor which is synchronized to the MSE are deleted then that controller is automatically removed from MSE assignment or unsynchronized.

**Related Topics**

- Synchronizing Prime Infrastructure and MSE
- Viewing Synchronization History
Synchronizing Prime Infrastructure and MSE
Synchronizing Controllers with MSEs
Managing Third-Party Elements on MSEs
Out-of-Sync Alarms

Viewing MSE Synchronization Status

You can use the Synchronize Servers command in Prime Infrastructure to view the status of network design, controller, and event group synchronization with an MSE.

To view synchronization status, follow these steps:

---

**Step 1** Choose Services > Mobility Services > Synchronize Services.

**Step 2** From the left sidebar menu, choose Network Designs, Controllers, Event Groups, Wired Switches Third Party Elements, or Service Advertisements.

For each of the elements, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified server such as an MSE. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a provided server.

A green two-arrow icon does not indicate the NMSP connection status for a controller.

You can also view the synchronization status at Monitor > Maps > System Campus > Building > Floor where Building is the building within the campus and Floor is a specific floor in that campus building.

The MSE Assignment option on the left sidebar menu shows which MSE the floor is currently assigned to. You can also change MSE assignment from this page.

---

**Related Topics**
- Viewing MSEs
- Adding MSEs to Prime Infrastructure
- Synchronizing Prime Infrastructure and MSE
- Synchronizing Controllers with MSEs
- Viewing Synchronization History
- Out-of-Sync Alarms

Viewing Synchronization History

You can view the synchronization history for the last 30 days for an MSE. This is especially useful when automatic synchronization is enabled as alarms are automatically cleared. Synchronization History provides a summary of those cleared alarms.

The Synchronization History page on the Services tab is available only in the root virtual domain in Release 7.3.

To view synchronization history, choose Services > Synchronization History and click the column headers to sort the entries.
Related Topics

- Viewing MSEs
- Synchronizing Prime Infrastructure and MSE
- Synchronizing Controllers with MSEs
- Managing Third-Party Elements on MSEs
- Setting and Verifying the Controller Time Zones
- Configuring Smart Mobility Services Engine Database Synchronization
- Out-of-Sync Alarms
- Viewing MSE Synchronization Status

Viewing MSE Notification Statistics

You can view the notification statistics for a specific MSE. To view the Notification Statistics for a specific MSE:

Choose Services > Mobility Services > Mobility Services Engines > MSE-name > Context Aware Service > Notification Statistics (where MSE-name is the name of an MSE).

Table 55-3 describes the fields in the Notification statistics page.

<table>
<thead>
<tr>
<th>Table 55-3 Notification Statistics Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td>Destinations</td>
</tr>
<tr>
<td>Total</td>
</tr>
<tr>
<td>Unreachable</td>
</tr>
<tr>
<td><strong>Notification Statistics Summary</strong></td>
</tr>
<tr>
<td>Destination Address</td>
</tr>
<tr>
<td>Destination Port</td>
</tr>
<tr>
<td>Destination Type</td>
</tr>
<tr>
<td>Destination Status</td>
</tr>
<tr>
<td>Last Sent</td>
</tr>
<tr>
<td>Last Failed</td>
</tr>
<tr>
<td>Track Definition (Status)</td>
</tr>
<tr>
<td>Total Count</td>
</tr>
</tbody>
</table>
Editing MSE General Properties for MSE

You can use Prime Infrastructure to edit the general properties of an MSE registered in Prime Infrastructure database. General properties include contact name, username, password, and HTTP.

To edit the general properties of an MSE, follow these steps:

**Step 1** Choose **Services > Mobility Services >Mobility Services Engines** to display the Mobility Services page.

**Step 2** Click the name of the MSE that you want to edit. The General Properties page (with a General tab and Performance tab) appears.

**Step 3** In the General Properties page, modify the following Server Details as necessary:

- **Contact Name**—Enter a contact name for the mobility service.
- **Username**—Enter the log in username for the Prime Infrastructure server that manages the mobility service.
- **Password**—Enter the log in password for the Prime Infrastructure server that manages the mobility service.
- **HTTP**—Select the **HTTP enable** check box to enable HTTP. When you have a non-default port or HTTPS turned on, you must pass the correct information along with the command. For example, `getserverinfo` must include `-port <<port>> -protocol <<HTTP/HTTPS>>`. Similarly, for stopping the server, `stoplocserver -port <<port>> -protocol <HTTP/HTTPS>`.
- **Legacy Port**—8001
- **Legacy HTTPS**—Select the check box to enable the legacy HTTPS.
- **Delete synchronized service assignments and enable synchronization**—Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the MSE. This option shows up only if the delete synchronized service assignments check box was unselected while adding an MSE.

Prime Infrastructure always uses HTTPS to communicate with an MSE.

The following tcp ports are in use on the MSE in Release 6.0: tcp 22: MSE SSH port, tcp 80: MSE HTTP port, tcp 443: MSE HTTPS port, tcp 1411: AeroScout, tcp 1999: AeroScout internal port, tcp 4096: AeroScout notifications port, tcp 5900X: AeroScout (X can vary from 1 to 10), and tcp 8001: Legacy port. Used for location APIs.

The following udp ports are in use on the MSE in Release 6.0: udp 123: NTPD port (open after NTP configuration), udp 162: AeroScout SNMP, udp/tcp 4000X: AeroScout proxy (X can vary from 1 to 5), udp 12091: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 12092: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 32768: Location internal port, udp 32769: AeroScout internal port, and udp 37008: AeroScout internal port.

**Step 4** In the Mobility Services dialog box, select the **Admin Status** check box to enable the applicable (Context Aware Service, WIPS, Mobile Concierge Service, Location Analytics Service, Billboard service) service.

If you select Context Aware Service, then you must select a location engine to perform location calculation.

Choose either of the following:

- **Cisco Tag Engine**

or
• Partner Tag Engine

**Note** With MSE 6.0, you can enable multiple services (CAS and wIPS) simultaneously. Before Version 6.0, MSEs can only supported one active service at a time.

The Mobility Services dialog box also shows the following:

• Service Name
• Service Version
• Service Status
• License Type

Use the [Click here](#) link to view MSE licensing details.

**Step 5** Click **Save** to update Prime Infrastructure and mobility service databases.

**Step 6** Click the **Performance** tab to view a graph of CPU and memory utilization percentages.

---

## Editing NMSP Parameters for MSE

Network Mobility Services Protocol (NMSP) manages communication between the mobility service and the controller. Transport of telemetry, emergency, and RSSI values between the mobility service and the controller is managed by this protocol.

**Note**

- The NMSP parameter is supported in mobility services installed with Release 3.0 through 7.0.105.0. It is not supported on releases later than 7.0.105.0.
- NMSP replaces the LOCP term introduced in Release 3.0.
- Telemetry and emergency information is only seen on controllers and Prime Infrastructure installed with Release 4.1 software or greater and on mobility service engine running release 3.0 or later software.
- The TCP port (16113) that the controller and mobility service communicate over must be open (not blocked) on any firewall that exists between the controller and mobility service for NMSP to function.

The NMSP Parameters dialog box in Prime Infrastructure enables you to modify NMSP parameters such as echo and neighbor dead intervals as well as response and retransmit periods.

To configure NMSP parameters, follow these steps:

**Step 1** Choose **Services > Mobility Services > Mobility Services Engines**.

**Step 2** Click the name of the MSE whose properties you want to edit.

**Step 3** From the left sidebar menu, choose **Status > NMSP Parameters**.

**Step 4** Modify the NMSP parameters as appropriate.
Note: We do not recommend you change the default parameter values unless the network is experiencing slow response or excessive latency.

NMSP parameters include the following:

- **Echo Interval**—Defines how frequently an echo request is sent from a mobility service to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds. If a network is experiencing slow response, you can increase the values of the echo interval, neighbor dead interval and the response timeout values to limit the number of failed echo acknowledgments.

- **Neighbor Dead Interval**—The number of seconds that the mobility service waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent. The default value is 30 seconds. Allowed values range from 1 to 240 seconds. This value must be at least two times the echo interval value.

- **Response Timeout**—Indicates how long the mobility service waits before considering the pending request as timed out. The default value is one second. Minimum value is one (1). There is no maximum value.

- **Retransmit Interval**—Interval of time that the mobility service waits between notification of a response timeout and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.

- **Maximum Retransmits**—Defines the maximum number of retransmits that are done in the absence of a response to any request. The default setting is 5. Allowed minimum value is zero (0). There is no maximum value.

**Step 5** Click **Save** to update Prime Infrastructure and mobility service databases.

### Viewing Active Session Details for MSE

The Active Sessions dialog box in Prime Infrastructure enables you to view active user sessions on the MSE.

**Step 1** Choose **Services > Mobility Services > Mobility Services Engines**.

**Step 2** Click the name of the MSE.

**Step 3** From the left sidebar menu, choose **System > Active Sessions**.

Prime Infrastructure shows a list of active mobility service sessions. For every session, Prime Infrastructure shows the following information:

- Session identifier
- IP address from which the mobility service is accessed
- Username of the connected user
- Date and time when the session started
- Date and time when the mobility service was last accessed
How long the session was idle since the last access

Viewing Trap Destinations for MSE

The Trap Destinations dialog box of Prime Infrastructure enables you to specify which Prime Infrastructure or Cisco Security Monitoring, Analysis, and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the MSE.

To view a trap destination for an MSE, follow these steps:

1. Choose Services > Mobility Services > Mobility Services Engines.
2. Click the name of the MSE.
3. From the left sidebar menu, choose System > Trap Destinations.

Prime Infrastructure shows a list of current trap destinations including the following information:

- IP address
- Port No.
- Community
- Destination type
- SNMP Version

Use the Select a command drop-down list to add or delete a trap destination.

Adding Trap Destinations for MSE

To add a trap destination, follow these steps:

1. Choose Services > Mobility Services > Mobility Services Engines.
2. Click the name of the mobility service.
3. From the left sidebar menu, choose System > Trap Destinations.
4. Choose Add Trap Destination from the command drop-down list and click Go.

The New Trap Destination page appears.

5. Enter the following details (see Table 55-4).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address for the trap destination</td>
</tr>
<tr>
<td>Port No.</td>
<td>Port number for the trap destination. The default port number is 162.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>This field is not editable and has a value of Other.</td>
</tr>
<tr>
<td>Snmp Version</td>
<td>Select either v2c or v3.</td>
</tr>
</tbody>
</table>
Editing MSE General Properties for MSE

Step 6  Click Save to save the changes or Cancel to discard the changes.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Name</strong></td>
<td>Username for the SNMP Version 3.</td>
</tr>
<tr>
<td><strong>Security Name</strong></td>
<td>Security name for the SNMP Version 3.</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>HMAC-MD5</td>
</tr>
<tr>
<td></td>
<td>HMAC-SHA</td>
</tr>
<tr>
<td><strong>Authentication Password</strong></td>
<td>Authentication password for the SNMP Version 3.</td>
</tr>
<tr>
<td><strong>Privacy Type</strong></td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>CBC-DES</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-128</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-192</td>
</tr>
<tr>
<td></td>
<td>CFB-AES-256</td>
</tr>
<tr>
<td><strong>Privacy Password</strong></td>
<td>Privacy password for the SNMP Version 3.</td>
</tr>
</tbody>
</table>

The following set of fields appear only if you select v3 as the SNMP version.

The Advanced Parameters dialog box in Prime Infrastructure enables you to set the number of days events are kept, set session time out values, set an absent data interval cleanup interval, and enable or disable Advanced Debug. You can use Prime Infrastructure to modify troubleshooting parameters for an MSE.

To edit advanced parameters for an MSE, follow these steps:

**Step 1**  Choose Services > Mobility Services > Mobility Services Engines.
**Step 2**  Click the name of the mobility service whose properties you want to edit.
**Step 3**  From the left sidebar menu, choose System > Advanced Parameters.
**Step 4**  View or modify the advanced parameters as necessary.
  - General Information
  - Advanced Parameters

**Caution**  Because advanced debugging slows the mobility service down, enable advanced debugging only under the guidance of Cisco TAC personnel.

- Number of Days to keep Events—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.
– Session Timeout—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option appears dimmed.

• Cisco UDI
  – Product Identifier (PID)—The Product ID of the MSE.
  – Version Identifier (VID)—The version number of the MSE.
  – Serial Number (SN)—Serial number of the MSE.

• Advanced Commands
  – Reboot Hardware—Click to reboot the mobility service hardware. See the “Rebooting the MSE Hardware” section on page 55-xxiii for more information.
  – Shutdown Hardware—Click to turn off the mobility service hardware. See the “Shutting Down the MSE Hardware” section on page 55-xxiii for more information.
  – Clear Database—Click to clear the mobility services database. Unselect the Retain current service assignments in the Prime Infrastructure check box to remove all existing service assignments from Prime Infrastructure and MSE. The resources have to be reassigned from Services > Synchronize Services page. This option is selected by default.

Step 5 Click Save to update Prime Infrastructure and mobility service databases.

---

**Rebooting the MSE Hardware**

If you need to restart an MSE, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the name of the MSE that you want to reboot.

**Step 3** Click System.

**Step 4** Click Advanced Parameters.

**Step 5** In the Advanced Commands dialog box, click Reboot Hardware.

**Step 6** Click OK to confirm that you want to reboot the MSE hardware.

The rebooting process takes a few minutes to complete.

---

**Shutting Down the MSE Hardware**

If you need to shut down an MSE, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the name of the MSE that you want to shut down.

**Step 3** Click System.

**Step 4** Click Advanced Parameters.

**Step 5** In the Advanced Commands dialog box, click Shutdown Hardware.
Step 6 Click OK to confirm that you want to shut down the MSE.

Clearing the MSE Database

To clear an MSE configuration and restore its factory defaults, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the name of the MSE you want to configure.
Step 3 Click System.
Step 4 Click Advanced Parameters.
Step 5 In the Advanced Commands dialog box, unselect the Retain current service assignments in the Prime Infrastructure check box to remove all existing service assignments from Prime Infrastructure and MSE.

The resources have to be reassigned in the Services > Synchronize Services page. By default, this option is selected.
Step 6 In the Advanced Commands dialog box, click Clear Database.
Step 7 Click OK to clear the MSE database.

Configuring MSE Logging Options

You can use Prime Infrastructure to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the name of the MSE that you want to configure.
Step 3 Choose System > Logs. The advanced parameters for the selected MSE appear.
Step 4 Choose the appropriate options from the Logging Level drop-down list.

There are four logging options: Off, Error, Information, and Trace.

All log records with a log level of Error or preceding are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

Caution Use Error and Trace only when directed to do so by Cisco TAC personnel.

Step 5 Select the Enabled check box next to each element listed in that section to begin logging its events.
Step 6 Select the Enable check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.
Step 7  To download log files from the server, click **Download Logs**. See the **Downloading MSE Log Files** for more information.

Step 8  In the Log File group box, enter the following:

- The number of log files to be maintained in the MSE. You can maintain a minimum of 5 log files and a maximum of 20 log files in the MSE.
- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

Step 9  In the MAC Address Based Logging group box, do the following:

- Select the **Enable** check box to enable MAC address logging. By default, this option is disabled.
- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking **Remove**.

See the **MAC Address-based Logging** for more information on MAC Address-based logging.

Step 10  Click **Save** to apply your changes.

### MAC Address-based Logging

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

```
/opt/mse/logs/locserver
```

A maximum of 5 MAC addresses can be logged at a time. The Log file format for MAC address `aa:bb:cc:dd:ee:ff` is `macaddress-debug-aa-bb-cc-dd-ee-ff.log`

You can create a maximum of two log files for a MAC Address. The two log files might consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files that are not updated for more than 24 hours are pruned.

### Downloading MSE Log Files

If you need to analyze MSE log files, you can use Prime Infrastructure to download them to your system. Prime Infrastructure downloads a zip file containing the log files.

To download a .zip file containing the log files, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Services &gt; Mobility Services &gt; Mobility Services Engines</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the name of the MSE to view its status.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>Logs</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Download Logs</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.</td>
</tr>
</tbody>
</table>

### Adding MSE Users

To add a users to an MSE, follow these steps:
Adding MSE Users

Step 1  Choose Services > Mobility Services > Mobility Services Engines.
Step 2  Click the device name of the MSE that you want to edit.
Step 3  From the left sidebar menu, choose Systems > Accounts > Users.
Step 4  From the Select a command drop-down list, choose Add User.
Step 5  Click Go.
Step 6  Enter the username in the Username text box.
Step 7  Enter a password in the Password text box.
Step 8  Enter the name of the group to which the user belongs in the Group Name text box.
Step 9  Choose a permission level from the Permission drop-down list.

| Caution | Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access, that user is unable to configure MSE settings. |

Step 10  Click Save to add the new user to the MSE.

Deleting MSE Users

To delete a user from an MSE, follow these steps:

Step 1  Choose Services > Mobility Services > Mobility Services Engines.
Step 2  Click the device name of the MSE that you want to edit.
Step 3  From the left sidebar menu, choose Systems > Accounts > Users.
Step 4  Select the check box(es) of the user(s) that you want to delete.
Step 5  From the Select a command drop-down list, choose Delete User.
Step 6  Click Go.
Step 7  Click OK to confirm that you want to delete the selected users.

Editing User Properties

To change user properties, follow these steps:

Step 1  Choose Services > Mobility Services > Mobility Services Engines.
Step 2  Click the device name of the MSE that you want to edit.
Step 3  From the left sidebar menu, choose Systems > Accounts > Users.
Step 4  Click the username of the user that you want to edit.
Adding User Groups

To add a user group to an MSE, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the device name of the MSE that you want to edit.

**Step 3** From the left sidebar menu, choose Systems > Accounts > Groups.

**Step 4** From the Select a command drop-down list, choose Add Group.

**Step 5** Click Go.

**Step 6** Enter the name of the group in the Group Name text box.

**Step 7** Choose a permission level from the Permission drop-down list.

There are three permissions levels to choose from:

- **Read Access**
- **Write Access**
- **Full Access** (required for Prime Infrastructure to access mobility services engines)

**Step 8** Click Save to add the new group to the MSE.

**Caution**

Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access permission, that user cannot configure MSE settings.

Deleting User Groups

To delete user groups from an MSE, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the device name of the MSE that you want to edit.

**Step 3** From the left sidebar menu, choose Systems > Accounts > Groups.

**Step 4** Select the check box(es) of the group(s) that you want to delete.

**Step 5** From the Select a command drop-down list, choose Delete Group.

**Step 6** Click Go.

**Step 7** Click OK to confirm that you want to delete the selected users.


Editing Group User Permissions

To change user group permissions, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Services &gt; Mobility Services &gt; Mobility Services Engines.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the device name of the MSE that you want to edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>Systems &gt; Accounts &gt; Groups.</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the group name of the group that you want to edit.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose a permission level from the Permission drop-down list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Save</strong> to apply your change.</td>
</tr>
</tbody>
</table>

Caution: Group permissions override individual user permissions. For example, if you give a user permission for full access and add that user to a group with read access, that user is unable to configure MSE settings.

Monitoring Status Information for MSEs

The System > Status page enables you to monitor server events, Prime Infrastructure alarms and events, and NMSP connection status for the MSE.

Viewing MSE Server Events

To view a list of server events, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Services &gt; Mobility Services &gt; Mobility Services Engines.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the name of the applicable MSE.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the left sidebar menu, choose <strong>System &gt; Status &gt; Server Events.</strong></td>
</tr>
</tbody>
</table>

The Status > Server Events page provides the following information:

- Timestamp—Time of the server event.
- Severity—Severity of the server event.
- Event—Detailed description of the event.
- Facility—The facility in which the event took place.

Viewing MSE Audit Logs

You can view the audit logs for User-triggered operations using the Audit Logs option available in an MSE. To view the audit logs, follow these steps:
Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the applicable MSE.

Step 3 From the left sidebar menu, choose System > Status > Audit Logs.

The Status > Audit Logs page provides the following information:

- Username—The Username which has triggered the audit log.
- Operation—The operation that has been performed by the User.
- Operation Status—The status of the operation and it can be SUCCESSFUL or FAILED.
- Invocation Time—The date and time at which the audit log was recorded for the specified operation.

## Viewing MSE Alarms

To view a list of Prime Infrastructure alarms, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose System > Status > Prime Infrastructure Alarms.

## Out-of-Sync Alarms

Out-of-sync alarms are of Minor severity (yellow) and are raised in response to the following conditions:

- Elements have been modified in Prime Infrastructure (the auto-sync policy pushes these elements).
- Elements have been modified in the MSE.
- Elements except controllers exist in the MSE database but not in Prime Infrastructure.
- Elements have not been assigned to any MSE (the auto-sync policy does not apply).

Out-of-sync alarms are cleared when the following occurs:

- The MSE is deleted
  When you delete an MSE, the out-of-sync alarms for that system is also deleted. In addition, if you delete the last available MSE, the alarms for "elements not assigned to any server" are also deleted.
- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms might reappear the future when the scheduled task is next executed)

By default, out-of-sync alarms are enabled. You can disable them in Prime Infrastructure by choosing Administration > System Settings > Alarms and Events > Scheduled Tasks, clicking Mobility Service Synchronization, unselecting the Auto Synchronization check box, and clicking Submit.
### Viewing MSE Events

To view a list of Prime Infrastructure events, follow these steps:

1. **Step 1**: Choose `Services > Mobility Services > Mobility Services Engines`.
2. **Step 2**: Click the name of the applicable mobility service.
3. **Step 3**: From the left sidebar menu, choose `System > Status > Prime Infrastructure Events`.

### Viewing MSE NMSP Connection Status

The NMSP Connection Status page allows you to verify the NMSP connection between the MSE and the Cisco controller to which the MSE is assigned.

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility service and the controller.

1. **Step 1**: Choose `Services > Mobility Services > Mobility Services Engines`.
2. **Step 2**: Click the name of the applicable mobility service.
3. **Step 3**: From the left sidebar menu, choose `System > Status > NMSP Connection Status`.

The NMSP Connection Status page shows the following information:

- **Summary**—The Summary section shows each device type, the total number of connections, and the number of inactive connections.
- **NMSP Connection Status**—This group box shows the following:
  - IP address—Click the device IP address to view NMSP connection status details for this device. See the Viewing NMSP Connection Status Details for additional information.
  - Target Type—Indicates the device to which the NMSP connection is intended.
  - Version—Indicates the current software version for the device.
  - NMSP Status—Indicates whether the connection is active or inactive.
  - Echo Request Count—Indicates the number of echo requests that were sent.
  - Echo Response Count—Indicates the number of echo responses that were received.
  - Last Message Received—Indicates the date and time of the most recent message received.
4. **Step 4**: Verify that the NMSP Status is ACTIVE.
   - If active, you can view details on wired switches, controllers, and wired clients.
   - If not active, resynchronize Prime Infrastructure device and the MSE.

You can launch an NMSP troubleshooting tool for an inactive connection.

### Viewing NMSP Connection Status Details

To view NMSP Connection Status details, follow these steps:
### Step 1
Choose **Services > Mobility Services > Mobility Services Engines**.

### Step 2
Click the name of the applicable mobility service.

### Step 3
From the left sidebar menu, choose **System > Status > NMSP Connection Status**.

### Step 4
Click the device IP address to open the NMSP Connection Status Details page. The Details page shows the following information:

- **Summary**
  - IP Address
  - Version—The current software version for the device.
  - Target Type—The device to which the NMSP connection is intended.
  - NMSP Status—Indicates whether the connection is active or inactive.
  - Echo Request Count—The number of echo requests that were sent.
  - Echo Response Count—The number of echo responses that were received.
  - Last Activity Time—The date and time of the most recent message activity between the device and the MSE.
  - Last Echo Request Message Received At—The date and time the last echo request was received.
  - Last Echo Response Message Received At—The date and time the last echo response was received.
  - Model—The device model.
  - MAC Address—The MAC address of the device, if applicable.
  - Capable NMSP Services—Indicates the NMSP-capable services for this device such as ATTACHMENT or LOCATION.

- **Subscribed Services**—Indicates subservices for each subscribed NMSP service. For example, MOBILE_STATION_ATTACHMENT is a subservice of ATTACHMENT.

- **Messages**
  - Message Type—Message types might include: ATTACHMENT_NOTIFICATION, ATTACHMENT_REQUEST, ATTACHMENT_RESPONSE, CAPABILITY_NOTIFICATION, ECHO_REQUEST, ECHO_RESPONSE, LOCATION_NOTIFICATION, LOCATION_REQUEST, SERVICE_SUBSCRIBE_REQUEST, SERVICE_SUBSCRIBE_RESPONSE.
  - In/Out—Indicates whether the message was an incoming or outgoing message.
  - Count—Indicates the number of incoming or outgoing messages.
  - Last Activity Time—The date and time of the most recent activity or message.
  - Bytes—Size of the message in Bytes.

---

**Editing MSE Backup Parameters**

To view or edit mobility service backup parameters, follow these steps:

### Step 1
Choose **Services > Mobility Services > Mobility Services Engines**.
Monitoring Status Information for MSEs

Chapter 55  Cisco Mobility Services Engine and Services

Step 2  Click the name of the mobility service whose properties you want to edit.

Step 3  From the left sidebar menu, choose Maintenance > Backup.
- Backups located at—Indicates the location of the backup file.
- Enter a name for the Backup—Enter or edit the name of the backup file.
- Timeout (in secs)—Indicates the length of time (in seconds) before attempts to back up files times out.

Backing Up MSE Historical Data

Prime Infrastructure contains functionality for backing up MSE data.

Step 1  Choose Services > Mobility Services > Mobility Services Engines.

Step 2  Click the name of the MSE that you want to back up.

Step 3  From the left sidebar menu, choose Maintenance > Backup.

Step 4  Enter the name of the backup.

Step 5  Enter the time in seconds after which the backup times out.

Step 6  Click Submit to back up the historical data to the hard drive of the server running Prime Infrastructure.

Status of the backup can be seen on the page while the backup is in process. Three items are displayed on the page during the backup process: (1) Last Status field provides messages noting the status of the backup; (2) Progress field shows what percentage of the backup is complete; and (3) Started at field shows when the backup began noting date and time.

You can run the backup process in the background while working on other MSE operations in another Prime Infrastructure page.

Backups are stored in the FTP directory that you specify during the Prime Infrastructure installation. However, in the Prime Infrastructure installation, the FTP directory is not specified. It might be necessary to provide the full path of the FTP root.

Restoring MSE Historical Data

To restore a file back into the mobility service, follow these steps:

Step 1  Choose Services > Mobility Services > Mobility Services Engines.

Step 2  Click the name of the mobility service whose properties you want to edit.

Step 3  From the left sidebar menu, choose Maintenance > Restore.

Step 4  Choose the file to restore from the drop-down list.

Step 5  Select the Delete synchronized service assignments check box if you want to permanently remove all service assignments from the MSE.

This option is applicable for network designs, wired switches, controllers and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.
Step 6 Click Submit to start the restoration process.

Step 7 Click OK to confirm that you want to restore the data from the Prime Infrastructure server hard drive. When the restoration is complete, Prime Infrastructure shows a message to that effect.

You can run the restore process in the background while working on other MSE operations in another Prime Infrastructure page.

## Downloading Software to MSEs

To download software to an MSE using Prime Infrastructure, follow these steps:

**Step 1** Verify that you can ping the location appliance from Prime Infrastructure or an external FTP server, whichever you are going to use for the application code download.

**Step 2** Choose Services > Mobility Services > Mobility Services Engines.

**Step 3** Click the name of the MSE to which you want to download software.

**Step 4** On the left sidebar menu, choose Maintenance.

**Step 5** Click Download Software and do one of the following:

- To download software listed in Prime Infrastructure directory, select the **Select from uploaded images to transfer into the Server** check box. Then, choose a binary image from the drop-down list.

  Prime Infrastructure downloads the binary images listed in the drop-down list into the FTP server directory you specified during the Prime Infrastructure installation.

  In the Prime Infrastructure installation, FTP directory is not specified. It might be necessary to give the full path of the FTP root.

- To use downloaded software available locally or over the network, select the **Browse a new software image to transfer into the Server** check box and click Browse. Locate the file and click Open.

**Step 6** Enter the time, in seconds (between 1 and 1800), after which the software download times out.

**Step 7** Click Download to send the software to the /opt/installers directory on the MSE.

## Configuring Partner Systems for MSEs

The System > Partner Systems page enables you to do MSE-Qualcomm PDS configuration. This configuration is aimed at providing better navigation capability for the mobile devices. The Partner Discovery Server (PDS) generates encrypted assistance data using the floor plan and AP data which is provided by the MSE. The PDS converts this information into an optimized format that will be used by Qualcomm smart phones.

### Configuring Qualcomm PDS for MSE

To configure Qualcomm PDS for MSE, follow these steps:
Step 1  Choose **Services > Mobility Services > Mobility Services Engines**.

Step 2  Click the name of the mobility services.

Step 3  From the left sidebar menu, choose **System > Partner Systems**.

   The Qualcomm PDS Configuration for MSE page appears.

Step 4  If you want to enable MSE-Qualcomm communication, then select the **Enable Qualcomm** check box.

Step 5  In the Qualcomm PDS Endpoint text box, enter the Qualcomm PDS server URL. This is the URL of the PDS from where you can fetch data assistance. The default URL is

   `http://207.114.133.174:8000/AssistanceDataMgr/AssistanceDataMgrSOAP?wsdl`

Step 6  In the MSE URL to request assistance data text box, enter the MSE URL. This is the URL at which the MSE is accessible by the devices at the venue.

Step 7  In the Cisco Mobile Concierge SSID text box, enter the Mobile Concierge SSID information of the venue to which mobile clients should connect. The Qualcomm smart phones will associate this SSID and communicate with MSE.

Step 8  Enter the venue description in the **Venue Description** text box.

Step 9  Enter refresh time period for assistance data for MSE in the **Refresh time period for assistance data on MSE text box**.

Step 10 Enter refresh time period for assistance data for mobile clients in the **Refresh time period for assistance data on mobile clients text box**.

Step 11 Select the Include Copyright Information check box if the messages/assistance data sent to Qualcomm PDS server and mobile clients should be copyrighted.

Step 12 In the **Copyright Owner** text box, enter the copyright owner information that has to be included.

Step 13 Enter the copyright year to be included in the **Copyright Year** text box.

Step 14 Click **Save** to save the configuration and **Cancel** to go back.

---

### MSE-Qualcomm Configuration

The MSE-Qualcomm configuration involves the following steps:

- Generate Map Extraction Tool (MET) output from CAD file.
- Input MET Output into Prime Infrastructure
- Addition of GPS Markers
- Synchronize the Floor to MSE
- Provide Qualcomm QUIPS/PDS and Copyright Information
- On MSE, perform F2 Interface request to Qualcomm PDS server

Qualcomm’s MET is an application that allows you to customize and select various layers from a map file (DXF file) and generates a zip file containing:

- Image file (.PNG format) to be used as floor map on Prime Infrastructure.
- Span.xml file that contains the dimensions of the floor (horizontal and vertical) in meters.
- Qualcomm specific map XML file containing geometric feature information related to walls, doors, points of interest, and so on.
Managing Context-Aware Service Software Parameters

Context-Aware Service (CAS) software allows an MSE to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature and asset availability about a client or tag (Cisco CX version or later) from Cisco access points.

CAS relies on two engines for processing the contextual information it receives. The Context-Aware Engine for Clients processes data received from Wi-Fi clients and the Context-Aware Engine for Tags processes data received from Wi-Fi tags; these engines can be deployed together or separately depending on the business need.

Mobility services engines do not track or map non-Cisco CX tags.
CAS was previously referred to as Cisco location-based services.

You can modify Context-Aware Service Software properties as to the type and number of clients or tags that are tracked and whether or not locations are calculated for those clients or tags.

You can also modify parameters that affect the location calculation of clients and tags such as Received Signal Strength Indicator (RSSI) measurements.

**Viewing Contextual Information**

Before you can use Prime Infrastructure to view contextual information, initial configuration for the MSE is required using a command-line interface (CLI) console session. See the *Cisco 3355 Mobility Services Engine Getting Started Guide* and the *Cisco 3100 MSE Getting Started Guide* at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

After its installation and initial configuration are complete, the MSE can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated Prime Infrastructure to communicate with each MSE to transfer and display selected data.

You can configure the MSE to collect data for clients, rogue access points, rogue clients, mobile stations, interferers, and active RFID asset tags.

**Licensing for Clients and Tags**

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.

- Licenses for tags and clients are offered separately.
- The clients license also contains tracking of rogue clients and rogue access points, and interferers (if enabled).
- Licenses for tags and clients are offered in a variety of quantities, ranging from 1,000 to 12,000 units.

The AeroScout Context-Aware Engine for Tags support 100 permanent tag licenses; Context-Aware Services consists of permanent tag licenses.

---

**Note**


---

**Context-Aware Service General Parameters**

To access the Context Aware Service > General page, choose Services > Mobility Services > Mobility Services Engines > General from the left sidebar menu. This page provides the following information:

- Version
- Operational Status
- Number of Tracked Wireless Clients
- Number of Traced Tags
- Number of Tracked Rogue APs
- Number of Tracked Rogue Clients
Managing Context-Aware Service Software Parameters

- Number of Tracked Interferers
- Number of Tracked Wired Clients
- Total Elements Tracked
- Tracked Elements (Wireless Clients, Rogue APs, Rogue Clients, Interferers, and Wired Clients) Limit
- Tracked Tags Limit

Clients represent a snapshot of client count every 15 minutes. Peak Clients is the peak count during that 15-minute time period. For example, in a 15-minute time period, the client count varies from 100 to 300. When Prime Infrastructure polls MSE, MSE returns the client count as the count at that exact time, which could be any number between 100 to 300, and the Peak Client Count as 300.

Modifying Tracking Parameters for Mobility Services

The MSE can track up to 25,000 clients or up to 25,000 tags (with the proper license purchase). Updates on the locations of elements being tracked are provided to the MSE from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable in Prime Infrastructure maps, queries, and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 25,000 element limit for clients or tags.

You can modify the following tracking parameters using Prime Infrastructure:

- Enable and disable element locations (client stations, active asset tags, interferers, wired clients, rogue clients, and rogue access points) you actively track.
  - Wired client location tracking enables servers in a data center to more easily find wired clients in the network. Servers are associated with wired switch ports in the network.
- Set limits on how many of specific elements you want to track.
  For example, given a client license of 12,000 trackable units, you can set a limit to track only 8,000 client stations (leaving 4,000 units available to track rogue clients and rogue access points). Once the tracking limit is met for a given element, the number of elements not being tracked is summarized in the Tracking Parameters page.
- Disable tracking and reporting of ad hoc rogue clients and access points.

To configure tracking parameters for an MSE, follow these steps:

**Step 1**  Choose Services > Mobility Services > Mobility Services Engines to open the Mobility Services page.

**Step 2**  Click the name of the MSE whose properties you want to edit. The General Properties page appears.

**Step 3**  Choose Context-Aware Software > Tracking Parameters from the Administration subheading to display the configuration options.

**Step 4**  Modify the following tracking parameters as appropriate (see Table 55-5).
### Tracking Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking Parameters</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the MSE.</td>
</tr>
<tr>
<td></td>
<td>In 7.0, the client license encompasses all network location service elements and is</td>
</tr>
<tr>
<td></td>
<td>shared among wireless clients, wired clients, rogue clients, access points, and</td>
</tr>
<tr>
<td></td>
<td>interferers.</td>
</tr>
<tr>
<td></td>
<td>The wired client limiting is supported from MSE 7.0 and Prime Infrastructure 1.0. In</td>
</tr>
<tr>
<td></td>
<td>other words, you can limit wired clients to a fixed number, say 500. This limit is</td>
</tr>
<tr>
<td></td>
<td>set to ensure that the licenses are not taken up completely by wired clients and some</td>
</tr>
<tr>
<td></td>
<td>licenses are available for other devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong> When upgrading the MSE from 6.0 to 7.0, if any limits have been set on</td>
</tr>
<tr>
<td></td>
<td>wireless clients or rogues, they reset because of the wired client limit change in 7.0.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of wired client stations</td>
</tr>
<tr>
<td></td>
<td>currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of wired client stations</td>
</tr>
<tr>
<td></td>
<td>beyond the limit.</td>
</tr>
<tr>
<td>Wired Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the MSE.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of client</td>
</tr>
<tr>
<td></td>
<td>stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive</td>
</tr>
<tr>
<td></td>
<td>value up to 25,000 which is the maximum number of clients that can be tracked by an MSE.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked clients is determined by the license purchased.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of client stations currently</td>
</tr>
<tr>
<td></td>
<td>being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of client stations beyond</td>
</tr>
<tr>
<td></td>
<td>the limit.</td>
</tr>
<tr>
<td>Wireless Clients</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of client stations by the MSE.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of client</td>
</tr>
<tr>
<td></td>
<td>stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive</td>
</tr>
<tr>
<td></td>
<td>value up to 25,000 which is the maximum number of clients that can be tracked by an MSE.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked clients is determined by the license purchased.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of client stations currently</td>
</tr>
<tr>
<td></td>
<td>being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of client stations beyond</td>
</tr>
<tr>
<td></td>
<td>the limit.</td>
</tr>
<tr>
<td>Rogue Access</td>
<td>1. Select the <strong>Enable</strong> check box to enable tracking of rogue clients and asset points</td>
</tr>
<tr>
<td>Points</td>
<td>by the MSE.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Enable Limiting</strong> check box to set a limit on the number of rogue</td>
</tr>
<tr>
<td></td>
<td>clients and asset tags stations to track.</td>
</tr>
<tr>
<td></td>
<td>3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive</td>
</tr>
<tr>
<td></td>
<td>value up to 25,000 which is the maximum number of rogue clients and access points that</td>
</tr>
<tr>
<td></td>
<td>can be tracked by an MSE.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The actual number of tracked rogues (clients and access points) is driven by</td>
</tr>
<tr>
<td></td>
<td>the client license purchased. The user must consider the number of clients that are</td>
</tr>
<tr>
<td></td>
<td>being tracked in determining the available quantity to allocate to track rogue clients</td>
</tr>
<tr>
<td></td>
<td>and access points because clients and rogue clients and access points are addressed by</td>
</tr>
<tr>
<td></td>
<td>the same license.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Active Value (Display only): Indicates the number of rogue clients and access</td>
</tr>
<tr>
<td></td>
<td>points currently being tracked.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Not Tracked (Display only): Indicates the number of rogue clients and access</td>
</tr>
<tr>
<td></td>
<td>points beyond the limit.</td>
</tr>
<tr>
<td>Exclude Ad-Hoc Rogues</td>
<td>Select the check box to turn off the tracking and reporting of ad hoc rogues in the</td>
</tr>
<tr>
<td></td>
<td>network. As a result, ad hoc rogues are not displayed on Prime Infrastructure maps or</td>
</tr>
<tr>
<td></td>
<td>its events and alarms reported.</td>
</tr>
</tbody>
</table>
Rogue Clients
1. Select the Enable check box to enable tracking of rogue clients by the MSE.
2. Select the Enable Limiting check box to set a limit on the number of rogue clients to track.
3. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of rogue clients that can be tracked by an MSE.

Note: The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.

Note: The actual number of tracked active RFID tags is determined by the license purchased.
### Table 55-5 Tracking Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Clients and Access Points</td>
<td>Select the <strong>Enable</strong> check box to enable rogue access point polling and enter the polling interval in seconds. Default value is 600. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)</td>
</tr>
<tr>
<td>Statistics</td>
<td>Select the <strong>Enable</strong> check box to enable statistics polling for the mobility service, and enter the polling interval in seconds. Default value is 900. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)</td>
</tr>
</tbody>
</table>

**Step 5** Click **Save** to store the new settings in the MSE database.

### Filtering Parameters for Mobility Services

You can limit the number of asset tags, wired clients, rogue clients, interferers and access points whose location is tracked by filtering on the following:

- **MAC addresses**
  
  Specific MAC addresses can be entered and labeled as allowed or disallowed from location tracking. You can import a file with the MAC addresses that are to be allowed or disallowed, or you can enter them individually in the Prime Infrastructure GUI page.

  The format for entering MAC addresses is `xx:xx:xx:xx:xx:xx`. If a file of MAC addresses is imported, the file must follow a specific format as follows:

  - Each MAC address should be listed on a single line.
  - Allowed MAC addresses must be listed first and preceded by an “[Allowed]” line item. Disallowed MAC addresses must be preceded by “[Disallowed].”
  - Wildcard listings can be used to represent a range of MAC addresses. For example, the first entry “00:11:22:33:*” in the Allowed listing that follows is a wildcard.

**Note**

Allowed MAC address formats are viewable in the Filtering Parameters configuration page. See Table 55-6 for details.

**EXAMPLE file listing:**

```
[Allowed]
00:11:22:33:*
22:cd:34:ae:56:45
02:23:23:34:*

[Disallowed]
00:10:*
ae:bc:de:ea:45:23
```

- **Probing clients**

  Probing clients are clients that are associated to another controller but whose probing activity causes them to be seen by another controller and be counted as an element by the “probed” controller as well as its primary controller.
Modifying Filtering Parameters

To configure filtering parameters for an MSE, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Services &gt; Mobility Services &gt; Mobility Services Engines. The Mobility Services page appears.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the name of the MSE whose properties you want to edit. The General Properties page appears.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the Context-Aware Software menu, choose Filtering Parameters from the Administration subheading to display the configuration options.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Modify the following filtering parameters as appropriate (see Table 55-6).</td>
</tr>
</tbody>
</table>

Table 55-6 Filtering Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Filtering Parameters</td>
<td></td>
</tr>
<tr>
<td>Duty Cycle Cutoff Interferers</td>
<td>Enter the duty cycle cutoff value for interferers so that only those interferers whose duty cycle meets the specified limits are tracked and counted against the Base location license. The default value for the Duty Cycle Cutoff Interferers is 0% and the configurable range is from 0% to 100%. To better utilize the location license, you can choose to specify a filter for interferers based on the duty cycle of the interferer.</td>
</tr>
<tr>
<td>MAC Filtering Parameters</td>
<td></td>
</tr>
<tr>
<td>Exclude Probing Clients</td>
<td>Select the check box to prevent location calculation of probing clients.</td>
</tr>
<tr>
<td>Enable Location MAC Filtering</td>
<td>1. Select the check box to enable MAC filtering of specific elements by their MAC address.</td>
</tr>
<tr>
<td></td>
<td>2. To import a file of MAC addresses (Upload a file for Location MAC Filtering field), browse for the filename and click Save to load the file. The imported list of MAC addresses auto-populates the Allowed List and Disallowed List based on their designation in the file.</td>
</tr>
<tr>
<td></td>
<td>Note To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering field.</td>
</tr>
<tr>
<td></td>
<td>3. To add an individual MAC address, enter the MAC addresses (format is xx:xx:xx:xx:xx:xx) and click either Allow or Disallow. The address appears in the appropriate column.</td>
</tr>
<tr>
<td></td>
<td>Note To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column.</td>
</tr>
<tr>
<td></td>
<td>Note To move multiple addresses, click the first MAC address and press Ctrl to highlight additional MAC addresses. Click Allow or Disallow based on its desired destination.</td>
</tr>
<tr>
<td></td>
<td>Note If a MAC address is not listed in the Allow or Disallow column, by default, it appears in the Blocked MACs column. If you click the Unblock button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by selecting the Disallow button under the Allow column.</td>
</tr>
</tbody>
</table>
**Modifying History Parameters for Mobility Services**

You can use Prime Infrastructure to specify how long to store (archive) histories on client stations, rogue clients, and asset tags. These histories are received from those controllers that are associated with the mobility service.

You can also program the mobility service to periodically remove (prune) duplicate data from its historical files to reduce the amount of data stored on its hard drive.

To configure mobility service history settings, follow these steps:

1. Choose Services > Mobility Services > Mobility Services Engines.
2. Click the name of the mobility service whose properties you want to edit.
3. From the left sidebar menu, choose Context Aware Service > History Parameters.
4. Modify the following history parameters as appropriate (see Table 55-7).
5. Click Save to store your selections in the location appliance database.

**Table 55-7 History Parameters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive for</td>
<td>Enter the number of days for the location appliance to retain a history of each enabled category. The default value is 30. Allowed values are from 1 to 99999.</td>
</tr>
<tr>
<td>Prune data starting at</td>
<td>Enter the number of hours and minutes at which the location appliance starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Enter the interval, in minutes, after which data pruning starts again (between 0, which means never, and 99900000). The default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes.</td>
</tr>
<tr>
<td>Enable History Logging of Location Transitions for</td>
<td>To enable history logging of Location transitions, choose one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>• Client Stations</td>
</tr>
<tr>
<td></td>
<td>• Wired Stations</td>
</tr>
<tr>
<td></td>
<td>• Asset Tags</td>
</tr>
<tr>
<td></td>
<td>• Rogue Clients</td>
</tr>
<tr>
<td></td>
<td>• Rogue Access Points</td>
</tr>
<tr>
<td></td>
<td>• Interferers</td>
</tr>
</tbody>
</table>

**Note** Before the mobility service can collect asset tag data from controllers, you must enable the detection of RFID tags using the `config rfid status enable` CLI command.

5. Click Save to store the new settings in the MSE database.
Enabling Location Presence for Mobility Services

You can enable location presence on the MSE to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by wireless and wired clients on a demand basis for use by location-based services and applications.

You can also import advanced location information such as the MAC address of a wired client and the wired switch slot and port to which the wired client is attached.

Location Presence can be configured when a new Campus, Building, Floor or Outdoor Area is being added or configured at a later date.

Once enabled, the MSE is capable of providing any requesting Cisco CX v5 client its location.

**Note**
Before enabling this feature, synchronize the MSE.

To enable and configure location presence on an MSE, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Select the MSE to which the campus or building or floor is assigned.

**Step 3** From the left sidebar menu, choose Context Aware Services > Administration > Presence Parameters.

**Step 4** Select the Service Type On Demand check box to enable location presence for Cisco CX clients v5.

**Step 5** Select one of the following Location Resolution options:

a. When Building is selected, the MSE can provide any requesting client, its location by building.
   - For example, if a client requests its location and the client is located in Building A, the MSE returns the client address as Building A.

b. When AP is selected, the MSE can provide any requesting client, its location by its associated access point. The MAC address of the access point appears.
   - For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the MSE returns the client address of 3034:00hh:0adg.

c. When X,Y is selected, the MSE can provide any requesting client, its location by its X and Y coordinates.
   - For example, if a client requests its location and the client is located at (50, 200) the MSE returns the client address of 50, 200.

**Step 6** Select any or all of the location formats:

a. Select the Cisco check box to provide location by campus, building and floor and X and Y coordinates. Default setting.

b. Select the Civic check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area.

c. Select the GEO check box to provide the longitude and latitude coordinates.

**Step 7** By default, the Location Response Encoding check box is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

**Step 8** Select the Retransmission Rule check box to allow the receiving client to retransmit the received information to another party.
Step 9  Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. The default value is 24 hours (1440 minutes).

Step 10  Click Save.

Importing Asset Information for Mobility Services

To import asset, chokepoint, and TDOA receiver information for the MSE using Prime Infrastructure, follow these steps:

Step 1  Choose Services > Mobility Services.
Step 2  Click the name of the MSE for which you want to import information.
Step 3  Choose Context Aware Service > Administration > Import Asset Information.
Step 4  Enter the name of the text file or browse for the filename.
Specify information in the imported file in the following formats:
- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname
Step 5  When the import filename is located in the Browse text box, click Import.

Exporting Asset Information for Mobility Services

To export asset, chokepoint, and TDOA receiver information from the MSE to a file using Prime Infrastructure, follow these steps:

Step 1  Choose Services > Mobility Services > Mobility Services Engines.
Step 2  Click the name of the MSE from which you want the export information.
Step 3  Choose Context Aware Service > Administration > Export Asset Information.
Information in the exported file is in the following formats:
- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname
Step 4  Click Export.
Click Open (display to screen), Save (to external PC or server), or Cancel (to cancel the request).
If you select Save, you are asked to select the asset file destination and name. The file is named assets.out by default. Click Close in the dialog box when the download is complete.

Importing Civic Information for Mobility Services

To import civic information for the MSE using Prime Infrastructure, follow these steps:
Managing Context-Aware Service Software Parameters

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the name of the MSE for which you want to import asset information.
Step 3 From the left sidebar menu, choose Context Aware Software.
Step 4 From the Administration left sidebar menu, choose Import Civic Information.
Step 5 Enter the name of the text file or browse for the filename.
   Information in the imported file should be one of the following formats:
   Switch IP Address, Slot Number, Port Number, Extended Parent Civic Address, X, Y, Floor ID, Building ID, Network Design ID, ELIN:"ELIN", PIDF-Lo-Tag:"Civic Address Element Value"
   Each entry must appear on a separate line.
Step 6 Click Import.

Context-Aware Service Wired Parameters

This section describes the Context Aware Service > Wired drop-down list parameters.

Monitoring Wired Switches

You can review details on the wired switch (IP address, MAC address, serial number, software version, and ELIN), its port, its wired clients (count and status), and its civic information.

Wired switch data is downloaded to the MSE through Prime Infrastructure when the Ethernet switch and the MSE are synchronized (Services > Synchronize Services > Switches). Communication between a location-capable switch and the MSE is over NMSP. Prime Infrastructure and the MSE communicate over XML.

To view details on wired switches, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the device name link of the appropriate wired location switch.
Step 3 Choose Context Aware Service > Wired > Wired Switches. A summary of wired switches that are synchronized with the MSE appears.
Step 4 See the Wired Switch Details for more information on the switch, its port, its wired clients (count and status), and its civic information click the IP address link.

Wired Switch Details

To view wired switch details, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the device name link of the appropriate MSE.
Step 3 Choose Context Aware Service > Wired > Wired Switches. A summary of wired switches that are synchronized with the MSE appears.
Step 4 Click the IP address link for the applicable wired switch. The Wired Switch Details page appears. The Wired Switch Details page has four tabs: Switch Information, Switch Ports, Civic, and Advanced.

You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available in all four dashlets of the Wired Switches page.

The Wired Switch Details tabs show the following information:

- Switch Information—Displays a total count summary of wired clients connected to the switch along with the state of the client (connected, disconnected, and unknown).
  - Connected clients—Clients that are connected to the wired switch.
  - Disconnected clients—Clients that are disconnected from the wired switch.
  - Unknown clients—Clients are marked as unknown when the NMSP connection to the wired switch is lost.

You can view detailed wired client information by clicking in one of the client count links (total clients, connected, disconnected, and unknown). See the “Monitoring Wired Clients” section on page 55-xlvi section for more information.

- Switch Ports—Displays a detailed list of the ports on the switch.

  You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, port type, and port number by clicking in the respective column heading.

- Civic—Displays a detailed list of the civic information for the wired switch.

- Advanced—Displays a detailed list of the additional civic information for the wired switch.

---

**Monitoring Wired Clients**

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, VLAN ID, and VLAN ID), port association, and its civic information.

Wired client data is downloaded to the MSE through Prime Infrastructure when the switch and the MSE are synchronized (Services > Synchronize Services > Switches).

Prime Infrastructure and the MSE communicate over XML.

You can view the details of the wired client on either the wired switches page (Context Aware Service > Wired > Wired Switches) or wired clients page (Context Aware Service > Wired > Wired Clients).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the search field on the wired clients page.

- If you want to examine wired clients as they relates to a specific switch, you can view that information on the wired switches page. See the Monitoring Wired Switches section for more information.

To view details on a wired client, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the device name link of the appropriate MSE.

**Step 3** Choose Context Aware Service > Wired > Wired Clients.

In the Wired Clients summary page, clients are grouped by their switch.

A client status is noted as connected, disconnected, or unknown:
Managing Context-Aware Service Software Parameters

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost. See the Viewing MSE NMSP Connection Status for more information about NMSP connections.

If you know the MAC address of the wired client, you can click that link to reach the detail page of the client or use the search field. See the Wired Client Details for more information on wired client details.

- You can also search for a wired client by its IP address, username, or VLAN ID.

If you click the IP address of the switch, you are forwarded to the detail page of the switch. See the Monitoring Wired Switches section for more information.

**Step 4** Click the MAC Address for the applicable client to view wired client details. See the Wired Client Details for more information on wired client details.

---

## Wired Client Details

To view wired client details, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the device name link of the appropriate MSE.

**Step 3** Choose Context Aware Service > Wired > Wired Clients. A summary of wired clients that are synchronized with the MSE appears.

**Step 4** Click the MAC address link for the applicable wired client. The Wired Client Details page appears.

The Wired Client Details page has four tabs: Device Information, Port Association, Civic Address, and Advanced.

The Wired Switch Details tabs show the following information:

- **Device Information**—Display MAC and IP address, username, serial and model number, UDI, software version, VLAN ID, and VLAN name.
- **Port Association**—Displays the physical location of the switch port/slot/module on which the wired client terminates, the client status (connected, disconnected, unknown), and the switch IP address.
- **Civic Address**—Displays any civic address information.
- **Advanced**—Displays extended physical address details for the wired clients, if applicable.

A client takes on the civic address and advanced location information that is configured for the port on which the client terminates. If no civic and advanced information is defined for the its port (port/slot/module) then no location data is displayed.

---

### Context-Aware Service Advanced Parameters

#### Modifying Northbound Notifications

Northbound notifications define which tag notifications the MSE sends to third-party applications.
To configure northbound parameters, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the name of the MSE you want to configure.

**Step 3** Choose Context Aware Service > Advanced > Notification Parameters to display the configuration options.

**Step 4** Select the Enable Northbound Notifications check box to enable the function.

**Step 5** Select the Notification Contents check box to send notifications to third-party applications (northbound).

**Step 6** Select one or more of the Notification Contents check boxes.

**Step 7** Select the Notification Triggers check box.

**Step 8** Select one or more of the Notification Triggers check boxes

**Step 9** Enter the IP address or hostname and port for the system that is to receive the northbound notifications.

**Step 10** Choose the transport type from the drop-down list.

**Step 11** Select the HTTPS check box if you want to use HTTPS protocol for secure access to the destination system.

**Step 12** To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of this page. See Table 55-10.

### Table 55-8 User-Configurable Conditional and Northbound Notifications Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Enter the rate, in milliseconds, at which the MSE generates notifications. A value of 0 (default) means that the MSE generates notifications as fast as possible (Northbound notifications only).</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>Enter the event queue limit for sending notifications. The MSE drops any event above this limit.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of times to generate an event notification before the refresh time expires. This parameter can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification may be lost in transit. Default value is 1.</td>
</tr>
<tr>
<td>Refresh Time</td>
<td>Enter the wait time in minutes that must pass before a notification is resent. For example, if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. Default value is 0 minutes.</td>
</tr>
<tr>
<td>Drop Oldest Entry on Queue Overflow</td>
<td>(Read-only). The number of event notifications dropped from the queue since startup.</td>
</tr>
<tr>
<td>Serialize Events per Mac address per Destination</td>
<td>Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.</td>
</tr>
</tbody>
</table>

**Step 13** Click Save.
Modifying Location Parameters for Mobility Services

You can use Prime Infrastructure to specify whether the mobility service retains its calculation times and how soon the mobility service deletes its collected Received Signal Strength Indicator (RSSI) measurement times. You can also apply varying smoothing rates to manage location movement of an element.

To configure location parameters, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the name of the mobility service whose properties you want to edit.

**Step 3** From the left sidebar menu, choose Context Aware Service > Location Parameters.

**Step 4** Modify the location parameters as appropriate (see Table 55-9).

### Table 55-9 Location Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Enable Calculation Time</td>
<td>Select the check box to enable the calculation of the time required to compute location.</td>
</tr>
<tr>
<td>Caution</td>
<td>Enable only under Cisco TAC personnel guidance because enabling this field slows down overall location calculations.</td>
</tr>
<tr>
<td>Enable OW Location</td>
<td>Select the check box to enable Outer Wall (OW) calculation as part of location calculation.</td>
</tr>
<tr>
<td>Note</td>
<td>The OW Location parameter is ignored by the location server.</td>
</tr>
<tr>
<td>Relative discard RSSI time</td>
<td>Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered stale and discarded. Default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended.</td>
</tr>
<tr>
<td>Absolute discard RSSI time</td>
<td>Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. Default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended.</td>
</tr>
<tr>
<td>RSSI Cutoff</td>
<td>Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), preceding which the mobility service always use the access point measurement. Default value is -75.</td>
</tr>
<tr>
<td>Note</td>
<td>When 3 or more measurements are available preceding the RSSI cutoff value, the mobility service discards any weaker values and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements following the RSSI cutoff value are available, those values are used for calculation.</td>
</tr>
<tr>
<td>Caution</td>
<td>Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation.</td>
</tr>
</tbody>
</table>
Click **Save** to store your selections in Prime Infrastructure and mobility service databases.

### Modifying Notification Parameters for Mobility Services

You can use Prime Infrastructure to configure MSE event notification parameters that define such items as how often the notifications are generated or resent by the MSE.

Modify notification parameters only if you expect the MSE to send a large number of notifications or if notifications are not being received.

You can also enable forwarding of northbound notifications for tags to be sent to third-party applications. The format of northbound notifications sent by the MSE is available on the Cisco developers support portal at the following URL:

---

**Table 55-9 Location Parameters (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Location Filtering</td>
<td>If enabled, the location filter is applied only for client location calculation. Enabling location filter allows previous location estimates to be used in estimating current location. This reduces location jitter for stationary clients and improve tracking for mobile clients.</td>
</tr>
<tr>
<td>Chokepoint Usage</td>
<td>Select the check box to enable the usage of chokepoint proximity to determine location. Applies to Cisco-compatible Tags capable of reporting chokepoint proximity.</td>
</tr>
<tr>
<td>Use Chokepoints for Interfloor conflicts</td>
<td>Allows the use of chokepoints to determine the correct floor during Interfloor conflicts. Choose <strong>Never</strong>, <strong>Always</strong>, or <strong>Floor Ambiguity</strong>.</td>
</tr>
<tr>
<td>Chokepoint Out of Range Timeout</td>
<td>After a Cisco-compatible Tag leaves a chokepoint proximity range, this is the timeout (in seconds) after which RSSI information is used again to determine location.</td>
</tr>
<tr>
<td>Absent Data Cleanup Interval</td>
<td>Enter the interval period (in minutes) for removing inactive elements from the database.</td>
</tr>
<tr>
<td>Use Default Heatmaps for Non Cisco Antennas</td>
<td>Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the Location Calculation. This option is disabled by default.</td>
</tr>
</tbody>
</table>

**Movement Detection**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual RSSI change threshold</td>
<td>This field specifies the Individual RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. Do not modify without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Aggregated RSSI change threshold</td>
<td>This field specifies the Aggregated RSSI movement recalculation trigger threshold. Enter a threshold value between 0-127 dBm. It should not be modified without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Many new RSSI change percentage threshold</td>
<td>This field specifies Many new RSSI movement recalculation trigger threshold in percentage. It should not be modified without Cisco TAC guidance.</td>
</tr>
<tr>
<td>Many missing RSSI percentage threshold</td>
<td>This field specifies Many missing RSSI movement recalculation trigger threshold in percentage. It should not be modified without Cisco TAC guidance.</td>
</tr>
</tbody>
</table>
To configure notification parameters, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobility Services Engines.

**Step 2** Click the name of the MSE you want to configure.

**Step 3** From the Context Aware Software left sidebar menu, choose Notification Parameters from the Advanced sub-heading to display the configuration options.

**Step 4** Select the Enable Northbound Notifications check box to enable the function.

**Step 5** Select the Notification Contents check box to send notifications to third-party applications (northbound).

**Step 6** Select one or more of the Notification content options.

**Step 7** Select the Notification Triggers check box.

**Step 8** Select one or more of the Notification trigger options.

**Step 9** Enter the IP address and port for the system that is to receive the northbound notifications.

**Step 10** Choose the transport type from the drop-down list.

**Step 11** Select HTTPS if you want to use HTTPS protocol for secure access to the destination system.

**Step 12** To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of the page. Table 55-10 describes each parameter.

### Table 55-10 User-Configured Conditional and Northbound Notifications Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Configuration Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Enter the rate in milliseconds at which the MSE generates notifications. A value of 0 (default) means that the MSE generates notifications as fast as possible (Northbound notifications only).</td>
</tr>
<tr>
<td>Queue Limit</td>
<td>Enter the event queue limit for sending notifications. The MSE drops any event preceding this limit.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of times to generate an event notification before the refresh time expires. This field can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification might be lost in transit. Default value is 1.</td>
</tr>
<tr>
<td>Refresh Time</td>
<td>Enter the wait time, in minutes, that must pass before a notification is resent. For example if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time.</td>
</tr>
<tr>
<td>Drop Oldest Entry on Queue Overflow</td>
<td>(Read-only). The number of event notifications dropped from the queue since startup.</td>
</tr>
<tr>
<td>Serialize Events per Mac address per Destination</td>
<td>Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.</td>
</tr>
</tbody>
</table>

**Step 13** Click Save.
Viewing Partner Engine Status

To access the Partner Engine Status page, choose Services > Mobility Services > Mobility Services Engines > MSE Name > Context Aware Service > Partner Engine > Status.

If tag licenses are available, then Aeroscout Tag Engine is enabled. Otherwise, Cisco Partner Engine is enabled by default.

If only the evaluation license is available, then the Cisco Partner Engine is enabled by default. The Partner Engine status page shows status based on whether it is a Aeroscout Tag Engine or Cisco Tag Engine.

Note

The Aeroscout engine fails to start on MSE if the Prime Infrastructure map names have special characters such as ‘&’.

Table 55-11 describes the fields in the Tag Engine Status page for the Aeroscout Tag Engine.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Location Engine Name</td>
<td>The Partner engine name, which is aeroscout.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the Aeroscout Tag Engine.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the Tag Engine.</td>
</tr>
<tr>
<td>Registered</td>
<td>Appears as True when the Aeroscout Tag Engine has established communication with the MSE.</td>
</tr>
<tr>
<td>Active</td>
<td>Appears as True when the Aeroscout Tag Engine is up and running.</td>
</tr>
<tr>
<td>License Information</td>
<td>The maximum tags that are available with the Aeroscout Tag Engine.</td>
</tr>
</tbody>
</table>

If you selected Cisco Tag Engine for Context Aware Service, the Tag Engine Status page displays the following information.

Table 55-12 describes the fields in the Tag Engine Status page for the Cisco Tag Engine.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Location Engine Name</td>
<td>The Tag location engine name, which is Cisco.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the Cisco Tag Engine.</td>
</tr>
<tr>
<td>Description</td>
<td>Description for the Cisco Tag Engine.</td>
</tr>
<tr>
<td>Active</td>
<td>Displays as True when the Cisco Tag Engine is up and running.</td>
</tr>
<tr>
<td>License Information</td>
<td>The maximum tags that are available with the Cisco Tag Engine.</td>
</tr>
</tbody>
</table>

Viewing MSE Notifications Summary

To view the Notification Summary, choose Services > Mobility Services > Context Aware Notifications > Notification Summary.
The mobility service sends event notifications and does not store them (fire and forget). However, if Prime Infrastructure is a destination of notification events, it stores the notifications it receives and groups them into the following seven categories:

- Absence (Missing)—Generated when the mobility service cannot see the asset in the WLAN for the specified time.
- Location Change Events—Generated when client stations, asset tags, rogue clients, and rogue access points move from their previous location.
- Chokepoint Notifications—Generated when a tag is seen (stimulated) by a chokepoint. This information is only reported and displayed for CCX v.1-compliant tags.
- Battery Level—Generated when a tracked asset tag hits the designated battery level.
- In/Out Area—Generated when an asset is moved inside or outside a designated area.
- Movement from Marker—Generated when an asset is moved beyond a specified distance from a designated marker you define on a map.
- Emergency—Generated for a CCX v.1 compliant asset tag when the panic button of the tag is triggered or the tag becomes detached, tampered with, goes inactive or reports an unknown state. This information is only reported and displayed for CCX v.1 compliant tags.

The summary details include the following:

- All Notifications
- Client Stations
- Asset Tags
- Rogue Clients
- Rogue Access Points

To view details for each of the notifications, click the number under the Last Hour, Last 24 Hours, or Total Active column to open the details page for the applicable notification.

Notifications Cleared

A mobility service sends event notifications when it clears an event condition in one of the following scenarios:

- Missing (Absence)—Elements reappear.
- In/Out Area (Containment)—Elements move back in or out of the containment area.
- Distance—Elements move back within the specified distance from a marker.
- Location Changes—Clear state is not applicable to this condition.
- Battery Level—Tags are detected again operating with Normal battery level.
- Emergency
- Chokepoint

In Prime Infrastructure, the Notifications Summary page reflects whether notifications for cleared event conditions have been received.
Viewing and Managing MSE Notifications

To view the Notification Definitions, choose Services > Mobility Services > Context Aware Notifications > Notification Definition. You can add event groups and event definitions to a group in this page. Every groups help you organize your event notifications. An event definition must belong to a particular group.

For more information on adding event groups and event definitions, see “Adding Event Groups” section on page 55-lvi and “Adding Event Definitions” section on page 55-lviii.

The Notification Definition page displays the following parameters only after adding event groups and event definitions:

Table 55-14 lists and describes the fields in the Notification Definition page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Name of the group to which the event definition is added.</td>
</tr>
<tr>
<td>Event Definitions</td>
<td>Existing event definitions for the event group.</td>
</tr>
<tr>
<td>Created On</td>
<td>Date on which the event groups are created.</td>
</tr>
</tbody>
</table>

Viewing Notification Statistics

You can view the notification statistics for a specific MSE. To view the Notification Statistics for a specific MSE, choose Services > Mobility Services > MSE-name > Context Aware Service > Notification Statistics (where MSE-name is the name of an MSE).

Table 55-14 lists and describes the fields in the Notification statistics page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>Destinations</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total count of the destinations.</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Count of unreachable destinations.</td>
</tr>
<tr>
<td>Notification Statistics Summary</td>
<td></td>
</tr>
<tr>
<td>Track Definition Status</td>
<td>Status of the track definition. Track notification status can be either Enabled or Disabled.</td>
</tr>
<tr>
<td>Track Definition</td>
<td>Track definition can be either Northbound or CAS event notification.</td>
</tr>
<tr>
<td>Destination IP Address</td>
<td>The destination IP address to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>The destination port to which the notifications are sent.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>The type of the destination. For example, SOAP_XML.</td>
</tr>
<tr>
<td>Destination Status</td>
<td>Status of the destination device. The status is either Up or Down.</td>
</tr>
<tr>
<td>Last Sent</td>
<td>The date and time at which the last notification was sent to the destination device.</td>
</tr>
</tbody>
</table>
Managing Context-Aware Service Software Parameters

Mobile Concierge Service Parameters

Viewing Configured Service Advertisements

To view the configured service advertisements, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Services &gt; Mobility Services &gt; Mobility Services Engines.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Device Name to view its properties.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Mobile Concierge Service &gt; Advertisements from the left sidebar menu.</td>
</tr>
</tbody>
</table>

The following information appears in the Mobile Concierge Service page:

- Icon—Displays an icon associated with the service provider.
- Provide Name—Displays the service provider name.
- Venue Name—Displays the venue name.
- Advertisements
  - Friendly Name—Friendly name that is displayed in the handset.
  - Advertisement Type—Type of advertisement that is displayed in the handset.

Viewing Mobile Concierge Service Statistics

To view Mobile Concierge service statistics, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Services &gt; Mobility Services &gt; Mobility Services Engines.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Device Name to view its properties.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Mobile Concierge service &gt; Statistics from the left sidebar menu.</td>
</tr>
</tbody>
</table>

The following information appears in the Mobile Concierge Service page:

- Top 5 Active Mobile MAC addresses—Displays information of the most active mobiles in a given venue.
- Top 5 Service URIs—Displays information of the usage of the services across a given venue or provider.

Table 55-14 Notification Statistics Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Failed</td>
<td>The date and time at which the notification had failed.</td>
</tr>
<tr>
<td>Total Count</td>
<td>The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.</td>
</tr>
</tbody>
</table>
Event Groups

To manage events more efficiently, you can use Prime Infrastructure to create event groups. Event groups help you organize your event definitions.

Adding Event Groups

To add an event group, follow these steps:

1. Choose Services > Mobility Services > Context Aware Notifications.
2. Choose Notification Definitions from the left sidebar menu.
3. From the Select a command drop-down list, choose Add Event Group.
4. Click Go.
5. Enter the name of the group in the Group Name text box.
6. Click Save.

The new event group appears in the Event Settings page.

Deleting Event Groups

To delete an event group, follow these steps:

1. Choose Services > Mobility Services > Context Aware Notifications.
2. Choose Notification Definitions from the left sidebar menu.
3. Select the check box of the event group you want to delete.
4. From the Select a command drop-down list, choose Delete Event Group(s).
5. Click Go.
6. Click OK to confirm the deletion.
7. Click Save.

Working with Event Definitions

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destinations. This section describes how to add, delete, and test event definitions.

Prime Infrastructure enables you to add definitions on a per-group basis. Any new event definition must belong to a particular group.

To add an event definition, follow these steps:
Step 1 Choose Services > Mobility Services > Context Aware Notifications.

Step 2 From the left sidebar menu, choose Notification Definitions.

Step 3 Click the name of the group to which you want to add the event. An event definition summary page appears for the selected event group.

Step 4 From the Select a command drop-down list, choose Add Event Definition.

Step 5 Click Go.

Step 6 Enter the name of the event definition in the Event Definition Name text box. The event definition name must be unique within the event group.

Step 7 Click Save.

Step 8 On the General tab, manage the following parameters:

- Admin Status—Enable event generation by selecting the Enabled check box (disabled by default).
- Priority—Set the event priority by choosing a number from the drop-down list. Zero is highest. An event definition with higher priority is serviced before event definitions with lower priority.
- Activate—To continuously report events, choose the All the Time check box. To indicate specific days and times for activation, unselect the All the Time check box and choose the applicable days and From/Until times. Click Save.

Step 9 On the Conditions tab, add one or more conditions. For each condition, specify the rules for triggering event notification. To add a condition, follow these steps:

  a. Click Add to open the Add/Edit Condition page.

  b. Choose a condition type from the Condition Type drop-down list and configure its associated Trigger If parameters see (Table 55-15).

<table>
<thead>
<tr>
<th>Condition Type</th>
<th>Trigger If</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing</td>
<td>Missing for Time (mins)—Enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the MSE generates a missing asset event if the MSE has not located the asset for more than 10 minutes.</td>
</tr>
<tr>
<td>In/Out</td>
<td>Inside of or Outside of—Click Select Area and choose the area parameters from the Select page. Click Select. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor).</td>
</tr>
<tr>
<td>Distance</td>
<td>In the distance of ( x ) (feet) from Marker text box—Enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker. Click Select Marker and choose the marker parameters in the Select page. Click Select.</td>
</tr>
<tr>
<td>Battery Level</td>
<td>Battery Level Is—Low, Medium, Normal. Select the appropriate battery level that triggers an event.</td>
</tr>
<tr>
<td>Location Change</td>
<td>An event is triggered if the location of the asset changes.</td>
</tr>
<tr>
<td>Emergency</td>
<td>Select Any, Panic Button, Tampered, or Detached check box.</td>
</tr>
<tr>
<td>Chokepoint</td>
<td>In the range of Chokepoints—Click Select Chokepoint check box and choose the chokepoint parameters in the Select page. Click Select.</td>
</tr>
</tbody>
</table>

  c. In the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients or Interferers) for which an event is generated if the trigger condition is met.
Emergency and chokepoint events are only applicable to tags (CCXv.1 compliant).

d. From the Match By drop-down list, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), the operator (Equals or Like), and enter the relevant text for the selected Match By element.

e. Click Add.

**Step 10** On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and configure the transport settings:

a. Click Add to open the Add/Edit Destination and Transport page.

b. To add one or more new destinations, click Add New, enter the applicable IP address, and click OK. The recipient system must have an event listener running to process notifications. By default, when you create an event definition, Prime Infrastructure adds its IP address as the destination.

c. To select a destination to receive notifications, click to highlight one or more IP addresses in the box on the right and click Select to add the IP address(es) to the box on the left.

d. From the Message Format field drop-down list, select XML or Plain Text. If you select Prime Infrastructure as the destination, you must select XML format.

e. Choose one of the following transport types from the Transport Type drop-down list:

   - SOAP—Simple Object Access Protocol. Use SOAP to send notifications over HTTP/HTTPS and to be processed by web services on the destination. Specify whether to send notifications over HTTPS by selecting its corresponding check box. Enter the destination port number in the Port Number text box.

   - Mail—Use this option to send notifications through e-mail. Choose the protocol for sending the e-mail from the Mail Type drop-down list. Enter the following: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.

   - SNMP—Simple Network Management Protocol. Use this option to send notifications to SNMP-capable devices. If you have selected SNMP version v2c then you are prompted to enter the SNMP community string in the SNMP Community text box and the applicable port number in the Port Number text box. If you have selected SNMP version v3 then you are prompted to enter the username, security name, choose the authentication type from the drop-down list, enter the authentication password, choose the privacy type from the drop-down list and enter the privacy password.

   - SysLog—Specifies the system log on the destination system as the recipient of event notifications. Enter the notification priority in the Priority text box, the name of the facility, and the port number on the destination system.

f. Click Add.

---

**Adding Event Definitions**

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destination.
Prime Infrastructure enables you to add definitions for each group. An event definition must belong to a group. See the Cisco Content-Aware Software Configuration Guide for more information on deleting or testing event definitions.

To add an event definition, follow these steps:

**Step 1** Choose Services > Mobility Services > Context Aware Notifications.

**Step 2** Choose Notification Definitions from the left sidebar menu.

**Step 3** Click the name of the group to which you want to add to the event. An event definition summary page appears for the selected event group.

**Step 4** From the Select a command drop-down list, choose Add Event Definition, and click Go.

**Step 5** On the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering event notifications.

**Tip** For example, to keep track of heart monitors in a hospital, you can add rules to generate event notifications when a heart monitor is missing for one hour, a heart monitor moves off its assigned floor, or a heart monitor enters a specific coverage area within a floor.

To add a condition, follow these steps:

a. Click Add to add a condition that triggers this event.

b. In the Add/Edit Condition dialog box, follow these steps:

1. Choose a condition type from the Condition Type drop-down list.
   
   If you chose Missing from the Condition Type drop-down list, enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the mobility service engine generates a missing asset event if the mobility service engine has not found the asset for more than 10 minutes. Proceed to Step c.

   If you chose In/Out from the Condition Type drop-down list, choose Inside of or Outside of, then select Select Area to select the area to monitor for assets going into it or out of it. In the Select dialog box, choose the area to monitor, then click Select. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor). For example, to monitor part of a floor in a building, choose a campus from the Campus drop-down list, choose a building from the Building drop-down list, choose the area to monitor from the Floor Area drop-down list. Then click Select. Proceed to Step c.

   If you chose Distance from the Condition Type drop-down list, enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker, then click Select Marker. In the Select dialog box, choose the campus, building, floor, and marker from the corresponding drop-down list, and click Select. For example, if you add a marker to a floor plan and set the distance in the Trigger. If the text box is set to 60 feet, an event notification is generated if the monitored asset moves more than 60 feet away from the marker. Proceed to Step c.

   You can create markers and coverage areas using the Map Editor. When you create marker names, make sure they are unique across the entire system.

   If you chose Battery Level from the Condition Type drop-down list, select the check box next to the battery level (low, medium, normal) that triggers an event. Proceed to Step c.

   If you chose Location Change from the Condition Type drop-down list, proceed to Step c.
If you chose Emergency from the Condition Type drop-down list, click the button next to the emergency (any, panic button, tampered, detached) that triggers an event. Proceed to Step c.

If you chose Chokepoint from the Condition Type drop-down list, proceed to Step c. There is only one trigger condition, and it is displayed by default. No configuration is required.

c. From the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients, or Interferers) for which an event is generated if the trigger condition is met.

If you choose the any option from the Apply to drop-down list, the battery condition is applied to all tags, clients, and rogue access points and rogue clients.

Emergency and chokepoint events apply only to Cisco-compatible extension tags Version 1 (or later).

d. From the Match By drop-down list, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), the operator (Equals or Like) from the drop-down list, and enter the relevant text for the selected Match By element.

Some examples of asset matching criteria that you can specify:

- If you choose MAC Address from the Match By drop-down list, choose Equals from the Operator drop-down list, and enter a MAC address (for example, 12:12:12:12:12:12), the event condition applies to the element whose MAC address is 12:12:12:12:12:12 (exact match).

- If you choose MAC Address from the Match By drop-down list, choose Like from the Operator drop-down list, and enter 12:12, the event condition applies to elements whose MAC address starts with 12:12.

e. Click Add to add the condition you have just defined.

If you are defining a chokepoint, you must select the chokepoint after you add the condition.

To select a chokepoint, do the following:

1. Click Select Chokepoint. An entry page appears.

2. Choose Campus, Building, and Floor from the appropriate drop-down lists.

3. Choose a Chokepoint from the menu that appears.

You are returned to the Add/Edit Condition page, and the location path (Campus > Building > Floor) for the chokepoint auto-populates the text area next to the Select Checkpoint button.

**Step 6**

On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and to configure the transport settings:

a. To add a new destination, click Add. The Add/Edit Destination configuration page appears.

b. Click Add New.

c. Enter the IP address of the system that receives event notifications, and click OK.

The recipient system must have an event listener running to process notifications. By default, when you create an event definition, Prime Infrastructure adds its IP address as the destination.

d. To select a destination to send event notifications to, highlight one or more IP addresses in the box on the right, and click Select to add the IP addresses to the box on the left.

e. Choose XML or Plain Text to specify the message format.

f. Choose one of the following transport types from the Transport Type drop-down list:

- **SOAP**—Specifies Simple Object Access Protocol, a simple XML protocol, as the transport type for sending event notifications. Use SOAP to send notifications over HTTP/HTTPS that are processed by web services on the destination.
If you choose SOAP, specify whether to send notifications over HTTPS by selecting its corresponding check box. If you do not, HTTP is used. Also, enter the destination port number in the Port Number text box.

- **Mail**—Use this option to send notifications through e-mail.
  
  If you choose Mail, you need to choose the protocol for sending the e-mail from the Mail Type drop-down list. You also need to enter the following information: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.

- **SNMP**—Use Simple Network Management Protocol, a very common technology for network monitoring used to send notifications to SNMP-capable devices.

  If you choose SNMP, enter the SNMP community string in the SNMP Community text box and the port number to send notifications to in the Port Number text box.

- **SysLog**—Specifies the system log on the destination system as the recipient of event notifications.

  If you choose SysLog, enter the notification priority in the Priority text box, the name of the facility in the Facility text box, and the port number of the destination system in the Port Number text box.

  g. To enable HTTPS, select the **Enable** check box next to it.
     
     Port Number auto-populates.

  h. Click **Save**.

**Step 7**

On the General tab, follow these steps:

a. Select the **Enabled** check box for Admin Status to enable event generation (disabled by default).

b. Set the event priority by choosing a number from the Priority drop-down list. Zero is the highest priority.

  An event notification with high priority is serviced before event definitions with lower priority.

  c. To select how often the event notifications are sent:
     
     1. Select the **All the Time** check box to continuously report events. Proceed to Step g.
     
     2. Unselect the **All the Time** check box to select the day and time of the week that you want event notifications sent. Days of the week and time fields appear for the selection. Proceed to Step d.

d. Select the check box next to each day you want the event notifications sent.

  e. Select the time for starting the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply From heading.

  f. Select the time for ending the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply Until heading.

  g. Click **Save**.

**Step 8**

Verify that the new event notification is listed for the event group (Mobility > Notifications > Settings > Event Group Name).

---

**Deleting an Event Definition**

To delete one or more event definitions from Prime Infrastructure, follow these steps:
Event Groups

Step 1  Choose Services > Mobility Services > Context Aware Notifications.
Step 2  From the left sidebar menu, choose Settings.
Step 3  Click the name of the group from which you want to delete the event definitions.
Step 4  Select the event definition that you want to delete by selecting its corresponding check box.
Step 5  From the Select a command drop-down list, choose Delete Event Definition(s).
Step 6  Click Go.
Step 7  Click OK to confirm that you want to delete the selected event definitions.

Searching for Wireless Client on MSE by IPv6 Address

Note Only wireless clients have IPv6 addresses in this release.

To search for an MSE located clients using the Prime Infrastructure Advanced search feature, follow these steps:

Step 1  Click Advanced Search.
Step 2  In the New Search dialog, choose Clients as the search category from the Search Category drop-down list.
Step 3  From the Media Type drop-down list, choose Wireless Clients.
The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.
Step 4  From the Wireless Type drop-down list, choose any of the following types: All, Lightweight or Autonomous Clients.
Step 5  From the Search By drop-down list, choose IP Address.
Searching a client by IP address can contain either full or partial IP address. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.
Step 6  From the Clients Detected By drop-down list, choose clients detected by as MSE.
This displays clients located by Context-Aware Service in the MSE by directly communicating with the controllers.
Step 7  From the Last detected within drop-down list, choose the time within which the client was detected.
Step 8  Enter the client IP address in the Client IP Address text box. You can enter wither a partial or full IPv6 address.
If you are searching for the client from Prime Infrastructure on the MSE by IPv4 address, enter the IPv4 address in the Client IP address text box.
Step 9  From the Client States drop-down list, choose the client states. The possible values for wireless clients are All States, Idle, Authenticated, Associated, Probing, or Excused. The possible values for wired clients are All States, Authenticated, and Associated.
Step 10 From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are All, unknown, Passed, and Failed.
Step 11  Select the CCX Compatible check box to search for clients that are compatible with Cisco Client Extensions. The possible values are All Versions, V1, V2, V3, V4, V5, and V6.

Step 12  Select the E2E Compatible check box to search for clients that are end-to-end compatible. The possible values are All Versions, V1, and V2.

Step 13  Select the NAC State check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are Quarantine, Access, Invalid, and Not Applicable.

Step 14  Select the Include Disassociated check box to include clients that are no longer on the network but for which Prime Infrastructure has historical records.

Step 15  From the Items per page drop-down list, choose the number of records to be displayed in the search results page.

Step 16  Select the Save Search check box to save the selected search option.

Step 17  Click Go.

The Clients and Users page appears with all the clients detected by the MSE.

---

**Viewing Clients Detected by MSE**

You can see the clients in probing state on 2.4 GHz on Cisco WLC but in probing state only on “a” radio (in the Monitor > Clients and Users > Client detected by MSE page). None of the clients shows up in probing state on “b/g” radio. This is because when clients are in the probing state, Prime Infrastructure does not get details on the protocol and by default these are shown to be on 5 GHz channel. After they are associated, the INFO messages are received from the controller which contain details on the protocol and the channel. But when they are probing with Measurement messages, Prime Infrastructure does not have this information and defaults it to 5 GHz.

To view all the clients detected by the MSE, follow these steps:

Step 1  Choose Monitor > Monitoring Tools > Clients and Users to view both wired and wireless clients information.

The Clients and Users table displays a few column by default. If you want to display the additional columns that are available, click Columns, and then click Columns. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

Step 2  Filter the current list to choose all the clients that are detected by the MSE by choosing Clients detected by MSE from the Show drop-down list.

All the clients detected by MSE including wired and wireless appear.

The following different parameters are available in the Clients Detected by MSE table:

- MAC Address—Client MAC address.
- IP Address—Client IP address.

The IP Address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:

- IPv4 address
Note

Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

- IPv6 global unique address. If there are multiple addresses of this type, most recent IPv6 address that the client received is shown, because a user could have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.
- IPv6 local unique address. If there are multiple IPv6 local unique addresses, then the most recent address appears.
- IPv6 link local address. For an IPv6 client it always have at least a link local address.

The following are the different IPv6 address types:
- Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.
- Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.
- Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses.

- IP Type—The IP address type can be IPv4 and IPv6.
  - Global Unique
  - Unique Local
  - Link Local
- User Name—Username based on 802.1x authentication. Unknown is displayed for client connected without a username.
- Type—Indicates the client type.
  - indicates a lightweight client
  - indicates a wired client
  - indicates an autonomous client
- Vendor—Device vendor derived from OUI.
- Device Name—Network authentication device name. For example, WLC and switch.
- Location—Map location of the connected device.
- VLAN—Indicates the access VLAN ID for this client.
- Status—Current client status.
  - Idle—Normal operation; no rejection of client association requests.
  - Auth Pending—Completing a AAA transaction.
  - Authenticated—802.11 authenticated complete.
  - Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.
  - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
- To Be Deleted—The client is deleted after disassociation.
- Excluded—Automatically disabled by the system due to perceived security threat.

- Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.
- Protocol
  - 802.11—wireless
  - 802.3—wired
- Association Time—Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network.
- CCX—Lightweight wireless only.

**Step 3** Select the radio button next to MAC Address in the Client and User page to view the associated client information.

### Viewing MSE Alarm Details

In the Monitor > Monitoring Tools > Alarms and Events page, click an MSE item under Failure Source column to access the alarms details for a particular MSE.

Alternatively, you can choose Services > Mobility Services Engines> MSE Name > System > Status > Prime Infrastructure Alarms page and click a particular MSE item under Failure Source column to access the alarms details for a particular MSE.

Table 55-16 describes the various fields in the Alarm Detail page for an MSE.

#### Table 55-16 General Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure Source</td>
<td>The MSE that generated the alarm.</td>
</tr>
<tr>
<td>Owner</td>
<td>Name of person to which this alarm is assigned, or blank.</td>
</tr>
<tr>
<td>Acknowledged</td>
<td>Displays whether or not the alarm is acknowledged by the user.</td>
</tr>
<tr>
<td>Category</td>
<td>The category of the alarm. The Alarm category is Mobility Services for MSEs.</td>
</tr>
<tr>
<td>Created</td>
<td>Month, day, year, hour, minute, second, AM or PM alarm created.</td>
</tr>
<tr>
<td>Modified</td>
<td>Month, day, year, hour, minute, second, AM or PM alarm last modified.</td>
</tr>
<tr>
<td>Generated By</td>
<td>This field displays MSE.</td>
</tr>
<tr>
<td>Severity</td>
<td>Level of security: Critical, Major, Minor, Warning, Clear, Info, Color coded.</td>
</tr>
</tbody>
</table>

The General information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information.

- Related Alarm List—Displays all the alarms related to a particular attack.
- Rogue Client Details—Displays information about the rogue clients.
- Annotations—Enter any new notes in this text box and click Add to update the alarm. Notes appear in the “Annotations” display page.
Monitoring with Mobile Concierge Services

The Mobile Concierge service allows the venue owners and service providers to monitor their WLAN. This solution delivers a unique in-store experience to customers who are using smart phones.

Mobile Concierge service uses wireless smart phones that have been configured with a set of policies for establishing network connectivity. Mobile Concierge service facilitates smartphones to discover network-based services available. Once you are connected to the stores Wi-Fi network, you can join the stores wireless guest network and can access variety of different services including electronic coupons, promotional offers, customer loyalty data, product suggestions, allow you to organize shopping lists, receive unique digital signature based on shopping preferences.

Related Topics

- Defining Venues
- Deleting Venues
- Defining Providers with Policies
- Deleting Providers
- Defining Policies
- Deleting Policies

Defining Venues

To define a venue, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobile Concierge.

**Step 2** Choose Mobile Concierge Services > Venues from the left sidebar menu.
The Venues page appears.

**Step 3**  
From the **Select a command** drop-down list, choose **Define New Venue** and click **Go**.

The Venue Wizard page appears.

**Step 4**  
Enter the venue name in the **Venue Name** text box and click **Next**.

**Step 5**  
In the **Floor/Outdoor Association** group box, you can configure the following:

- From the **Area Type** drop-down list, choose the area type where you want to display the service advertisement. The possible values are **Floor Area** and **Outdoor Area**.

  **Note**  
The Building, Floor Area, and Coverage Area drop-down lists are displayed only if you select Floor Area as the area type.

- From the **Campus** drop-down list, choose the campus name where you want to display the service advertisements.

- From the **Building** drop-down list, choose the building name where you want the advertisements to appear.

- From the **Floor** drop-down list, choose the floor type.

- From the **Coverage Area** drop-down list, choose the coverage area within the floor.

- From the **Outdoor Area** drop-down list, choose the outdoor area where you want to display the service advertisements. This field is displayed only if you select Outdoor Area as the Area Type.

**Step 6**  
Click **Next**. The Audio group box appears.

**Step 7**  
From the **Audio** group box, click **Choose File** to browse and select the audio file to play the audio notification.

**Step 8**  
Click **Next**. The Icons group box appears.

**Step 9**  
From the **Icons** group box, click **Choose File** to browse and select the icon that you want to display on the clients handset.

**Step 10**  
Click **Next**. The Venue Apps group box appears.

**Step 11**  
From the **Venue Apps** group box, choose the venue app on which you want to display the service advertisement from the **Web App** drop-down list.

**Step 12**  
Click **Next**. The Additional Venue Information group box appears.

**Step 13**  
From the **Additional Information** group box, you can provide any additional information that the venue would like to provide to the mobile application. You can configure the following:

- Enter the location detail in the **Location Detail** text box. This provides details such as store address, zip code, or street address of the venue.

- Enter the GPS latitude and longitude of the venue in the **Latitude** and **Longitude** text box. This helps the applications to identify the venue accurately.

- Enter any other additional information that the venue would like to provide to the mobile application in the **Additional Information** text box.

**Step 14**  
Click **Save**. This information is applied to the MSE and the synchronization happens automatically.

**Related Topics**

- Monitoring with Mobile Concierge Services
Deleting Venues

To delete a venue, follow these steps:

**Step 1**  Choose Services > Mobility Services > Mobile Concierge.
**Step 2**  Choose Mobile Concierge Services > Venues from the left sidebar menu.
The Venues page appears.
**Step 3**  Select the check box of the venue that you want to delete.
**Step 4**  From the Select a command drop-down list, choose Delete Venue, and click Go.
Click OK to confirm the deletion.

Related Topics
- Monitoring with Mobile Concierge Services
- Defining Venues
- Defining Providers with Policies
- Deleting Providers
- Defining Policies
- Deleting Policies

Defining Providers with Policies

**Step 1**  Choose Services > Mobility Services > Mobile Concierge.
**Step 2**  Choose Mobile Concierge Services > Providers from the left sidebar menu.
The Providers page appears.
**Step 3**  From the Select a command drop-down list, choose Define New Provider and click Go.
The Provider Wizard page appears.
**Step 4**  Enter the providers venue name in the Provider Name text box.
**Step 5**  Click Next. The Icons group box appears.
**Step 6**  From the Icons group box, click Choose File to browse and select the icon that you want to display on the clients handset.
**Step 7**  Click Next. The Local Services group box appears.
**Step 8**  From the Local Services group box, do the following:
• Click the inverted triangle icon location at the left side of the Local Service # name to expand the Local Service and configure the following:
  – Choose the service type from the Service Type drop-down list. The possible options are: Directory Info, Sign Up, Discount Coupon, Network Help, and Other.
  – Enter the display name in the Display Name text box.
  – Enter the description in the Description text box.
  – Choose the service URIs from the Service URIs drop-down list.
  – Enter the recommended application for the venue in the Recommended Apps text box.

**Step 9** Click Save.

---

**Related Topics**

- Monitoring with Mobile Concierge Services
- Deleting Providers
- Defining Venues
- Deleting Venues
- Defining Policies
- Deleting Policies

---

**Deleting Providers**

To delete a provider, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobile Concierge.
**Step 2** Choose Mobile Concierge Services > Providers from the left sidebar menu.

The Providers page appears.

**Step 3** Select the check box of the provider that you want to delete.
**Step 4** From the Select a command drop-down list, choose Delete Provider, and click Go.

Click OK to confirm the deletion.

---

**Related Topics**

- Monitoring with Mobile Concierge Services
- Defining Policies
- Defining Venues
- Deleting Venues
- Defining Providers with Policies
- Deleting Policies
Defining Policies

To define policies, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobile Concierge.

**Step 2** Choose Mobile Concierge Services > Policies from the left sidebar menu.

The Policies page appears.

**Step 3** From the Select a command drop-down list, choose Define New Policy and click Go.

The Policy Wizard page appears.

**Step 4** Choose the venue on which you want the policy to be applied from the Venue drop-down list.

**Step 5** Click Next. The Provider group box appears.

**Step 6** Choose the provider from the Provider drop-down list.

**Step 7** Click Next. The SSID group box appears.

**Step 8** From the SSID drop-down list, choose the SSIDs on which you want to broadcast the service advertisements and click OK. You can choose multiple SSIDs.

**Step 9** Click Next. The Display Rule group box appears.

**Step 10** From the Display Rule group box, you can do the following:

- Select the Display Rule radio button. You can select either Everywhere or Near selected APs radio button. By default, Display everywhere is selected.

If you select Display everywhere, then it searches for all the Mobile Concierge-supported controllers that provide these SSIDs and assigns these controllers to the MSE.

If you select Display near selected APs, then you can configure the following parameters:

- AP—Select those APs on which you want the advertisements to broadcast.
- Radio—Select the radio frequency on which you want the advertisements to be broadcasted. The service advertisement is displayed when the mobile device is near the radio band that you have selected. The possible values are 2.4 GHz or 5 GHz.
  - min RSSI—Enter a value for RSSI at which you want the service advertisements to be displayed on the user interface.

**Step 11** Click Finish.

Related Topics

- Monitoring with Mobile Concierge Services
- Deleting Policies
- Defining Venues
- Deleting Venues
- Defining Providers with Policies
- Deleting Providers
- Defining Policies
Deleting Policies

To delete a new policy, follow these steps:

**Step 1** Choose Services > Mobility Services > Mobile Concierge.

**Step 2** Choose Mobile Concierge Services > Policies from the left sidebar menu. The Policies page appears.

**Step 3** Select the check box of the policy that you want to delete.

**Step 4** From the Select a command drop-down list, choose Delete Policy, and click Go. Click OK to confirm the deletion.

**Related Topics**
- Monitoring with Mobile Concierge Services
- Defining Venues
- Deleting Venues
- Defining Providers with Policies
- Deleting Providers
- Defining Policies

Configuring and Deploying wIPS Solution Using the Wireless Security Configuration Wizard

The Wireless Security wizard page appears and allows you to perform the following wIPS related configurations:

- Allows rogue policy to detect and report ad hoc networks.
- Allows rogue rules to define rules to automatically classify rogue access points.
- Allows you to add new wIPS profiles.

**Step 1** Choose Services Mobility Services > Wireless Security.

By default, the Before You Begin tab opens. The Before You Begin wizard page displays information about how to use the Wireless Security wizard and includes the following information:

- Rogue Policy—The Rogue Policy page enables you to configure the rogue policy. It has three pre-configured rogue policy settings for rogue detection and containment.
- Rogue Rules—The Rogue Rules page allows you to automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. Rogue rules can be created to classify rogues as Malicious and Friendly.
• wIPS Profile—The wIPS Profile page provides several pre-defined profiles from which to choose. These profiles allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. The profile can be further customized by selecting the awIPS signatures to be detected and contained.

• Devices—The Devices page allows you to apply rogue policy, rogue rules, and wIPS profiles to controllers.

**Step 2** Click Next to configure the Rogue Policy to detect and report ad hoc networks. This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

• You can either set the policy settings to Low, High, or Critical by moving the Configure the rogue policy settings sliding bar with the mouse or select the Custom check box to configure the policy settings.

• In the General group box, configure the following fields:
  - Rogue Location Discovery Protocol—Determines whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following from the drop-down list:
    - Disable—Disables RLDP on all access points.
    - All APs—Enables RLDP on all access points.
    - Monitor Mode APs—Enables RLDP only on access points in monitor mode.
  - Expiration Timeout for Rogue AP and Rogue Client Entries—Set the expiration timeout (in seconds) for rogue access point entries. The valid range is 240 to 3600 seconds.
  - Validate rogue clients against AAA—Select the Validate rogue clients against AAA check box to enable the AAA validation of rogue clients.
  - Detect and report Adhoc networks—Select the Detect and report Adhoc networks check box to enable detection and reporting of rogue clients participating in ad hoc networking.
  - Rogue Detection Report Interval—In the Rogue Detection Report Interval text box, enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
  - Rogue Detection Minimum RSSI—In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBm to -128 dBm. This feature is applicable to all the AP modes.
  - Rogue Detection Transient Interval—In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

• In the Auto Contain group box, configure the following fields:
  - Rogue on Wire—Select the Rogue on Wire check box to auto contain those APs that are detected on the wired network.
  - Using our SSID—Select the Using our SSID check box.
  - Valid client on Rogue AP—Select the Valid client on Rogue AP check box to auto contain the valid clients from connecting to the rogue APs.
  - AdHoc Rogue—Select the AdHoc Rogue checkbox to auto contain adhoc rogue APs.
• Click Apply to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click Apply to Controllers.

**Step 3**
Click **Next** to configure the rogue rules. This page enables you to define rules to automatically classify rogue access points. Prime Infrastructure applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

**Step 4**
Click Create New to create new rogue rules. The Add/Edit Rogue Rule window appears.

• In the General group box, configure the following fields:
  - Rule Name—Enter a name for the rule in the text box.
  - Rule Type—Choose Malicious or Friendly from the drop-down list.

| Note | Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules. |

• Match Type—Choose Match All Conditions or Match Any Condition from the drop-down list.

• In the Rogue Classification Rule group box, configure the following fields:
  - Open Authentication—Select the Open Authentication check box to enable Open Authentication.
  - Match Managed AP SSID—Select the Match Managed AP SSID check box to enable the matching of managed AP SSID rule condition.
  - Match User Configured SSID (Enter one per line)—Select the Match User Configured SSID check box to enable the matching of user configured SSID rule condition.
  - Minimum RSSI—Select the Minimum RSSI check box to enable the Minimum RSSI threshold limit.
  - Time Duration—Select the Time Duration check box to enable the Time Duration limit.

| Note | Managed SSID are the SSIDs configured for the WLAN and is known to the system. |

| Note | User Configured SSID are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box. |

| Note | Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold. |

| Note | Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit. |

• Minimum Number Rogue Clients—Select the Minimum Number Rogue Clients check box to enable the Minimum Number Rogue Clients limit.
Note

Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

- Click Ok to save the rule or Cancel to cancel the creation or changes made to the current rule. You are returned to the Rogue Rules page and the newly added rogue rule is listed.
- Click Apply to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click Apply to Controllers.

Step 5
Click Next to configure the wIPS profiles. Prime Infrastructure provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile ‘as is’ or customize it to better meet your needs.

Step 6
For more information on configuring the wIPS profile, see the Configuring wIPS and Profiles section.

Step 7
After configuring wIPS profile, click Next to open the Devices page where you can select the controllers to apply the settings.
Configuring the Cisco AppNav Solution

Cisco AppNav is a hardware and software solution that simplifies network integration of WAN optimization. It also overcomes the challenges related to provisioning, visibility, scalability, asymmetry, and high availability.

- **Overview of Cisco AppNav**
- **Components of Cisco AppNav**
- **Prerequisites for Configuring Cisco AppNav**
- **Configuring Cisco AppNav**

### Overview of Cisco AppNav

The Cisco AppNav solution reduces the dependency on the intercepting switch or router by distributing the traffic among Cisco WAAS devices for optimization by using a powerful class and policy mechanism. You can use ISR-WAAS to optimize traffic based on sites or applications. This includes device-level and template-based configurations.

An intelligent load-balancing mechanism in the Cisco IOS-XE software allows the diversion of TCP traffic to various products, including Cisco WAAS and OneFirewall, where Cisco WAAS is the initial target. Router management is performed through the Cisco Prime Infrastructure network management application.

### Components of Cisco AppNav

The Cisco AppNav solution, is made up of a distribution unit called the Cisco AppNav Controller (AC), WAAS Service Nodes (SNs). The Cisco AppNav Controller distributes the flow, and the service nodes process the flows. You can group up to four Cisco AppNav-XE (routers) together to form a Cisco AppNav Controller Group (ACG) to support asymmetric flows and high availability. However, must ensure that all of the routers in the ACG are on the same platform and have the same memory capacity.

The Cisco AppNav solution's components perform the following functions:

- **AppNav Controller**—This is component that intelligently distributes traffic from a router to service nodes. The Cisco AppNav Controller is a part of Cisco IOS-XE Release 3.10 on the Cisco ISR-4400, Cisco CSR, and Cisco ASR 1K platforms.
- **Cisco WAAS Service Nodes**—These optimize traffic flows and are available in different form factors, for example, standalone appliances and virtualized ISR-WAAS running in a Cisco IOS-XE container.
Components of Cisco AppNav

- Cisco WAAS Central Manager—This is used to monitor and configure the ISR-WAAS.
- This chapter describes the configuration of the Cisco AppNav Controller functions on routers. Figure 56-1 describes the components of Cisco AppNav.

Figure 56-1 Components of Cisco AppNav

The advantages of using the Cisco AppNav components are:

- They can intelligently redirect new flows based on the load on each service node. This includes loads of individual application accelerators.
- If the flows do not require any optimization, service nodes can inform the Cisco AppNav Controller to directly pass the packets, thereby minimizing latency and resource utilization.
- There is minimal impact to traffic when adding or removing service nodes.
- The Cisco AppNav components support VRF. The VRF information is preserved when traffic returns from a service node. However, Prime Infrastructure does not support VRF.
- For specific applications, such as Messaging Application Programming Interface (MAPI) and Virtual desktop infrastructure (VDI), the components ensure that a family of flow is redirected to the same service node.
- Asymmetric flows can be optimized in situations where traffic in one direction goes through one Cisco AppNav Controller and the return traffic goes through a different Cisco AppNav Controller. But both redirect the traffic to the same ISR-WAAS. This is achieved using the Cisco AppNav Controller Group.
- Inter-box high availability is also supported using the Cisco AppNav Controller Group, which means that if one router goes down, traffic can be redirected to a different router in the Cisco AppNav Controller Group enabling uninterrupted flow.
Intra-box high availability of the Cisco AppNav Controller is supported on those Cisco ASR1000 Series platforms that have dual RP, or dual FP, or both. This means that if the active RP fails, the standby RP takes over or if the active FP fails, the standby FP takes over, and the flows continue uninterrupted.

The Cisco AppNav technology allows IP flows to be intercepted on routers and sent to a set of Cisco WAAS Service Node for processing. The initial application of Cisco AppNav which is supported in Cisco IOS-XE Release 3.10, is in Cisco WAAS.

**Prerequisites for Configuring Cisco AppNav**

The following are the prerequisites for configuring Cisco AppNav:

- The platform must be Cisco 4451-X ISR, Cisco Integrated Services Routers (ISR) G2, Cisco ASR 1000 Series Aggregation Services Routers, or Cisco Cloud Services Router.
- The software version of above mentioned platforms must be Version 3.10 and later.
- A valid appxk9 license must be enabled on the routers.
- A Cisco WAAS Service Node must be available.

**Configuring Cisco AppNav**

You must configure some parameters on the router before redirecting the traffic to the Cisco WAAS Service Node. If the Cisco AppNav configuration is generated as a part of installing the Cisco WAAS virtual appliance, it is transparent to the corresponding user. If it is configured using a template or through the Device Work Center, the user is more directly involved.

The Cisco AppNav can be configured in three ways:

- Configuring Cisco AppNav from the Device Work Center
- Configuring Cisco AppNav Using Templates
- Configuring Cisco AppNav Automatically During ISR-WAAS Container Activation

The Cisco AppNav configuration involves the use of the following:

- Controllers—A list of routers that cooperate to redirect traffic. This is a list of IP addresses, exactly one of which must belong to the router on which Cisco AppNav is being configured.
- Cisco WAAS Service Node Groups (SNGs)—There must be one or more SNGs that are the target of redirected traffic and are defined as a set of IP addresses.
- Class Maps—A set of class maps that classify incoming and outgoing traffic. Class maps consist of a set of match conditions that together specify traffic of interest. They can match traffic based on three types of conditions:
  - An access control list (ACL) that selects traffic based on a source and destination IP address and port.
  - A protocol that is used to select traffic that uses the Microsoft port mapper service rather than depending on fixed port numbers. This includes MAPI and a host of other Microsoft protocols.
  - A remote device that matches the traffic that has traversed a particular Cisco WAAS Service Node on the remote end. The remote device is identified by a MAC address.
• Policy maps—A Cisco AppNav policy map is an ordered list of rules, each of which specify what is to be done with some type of traffic. A rule thus consists of a class map and an action. The action is to either redirect to a service node group or to pass through.

• Clusters—A Cisco WAAS cluster is the combination of a policy map, controller group, and a set of service node groups used by the policy map. A cluster can be enabled or disabled. Prime Infrastructure allows several clusters to be defined but only one can be enabled at a time. An authentication key is used to secure communication between the controllers and the nodes in a cluster.

• Cisco WAAS interfaces—Traffic can be optimized only on interfaces where Cisco WAAS is enabled.

The WAN optimization template and the Device Work Center both have a default policy. The default policy consists of a number of class maps that match different types of traffic (HTTP, CIFS, TCP, and so on) that is optimized by Cisco ISR-WAAS. The template also includes a policy map containing a rule for each of those class maps. By default, all the matched traffic is redirected to a single service node group.

Configuring Cisco AppNav from the Device Work Center

The Device Work Center allows an administrator to view and modify the configuration of individual devices. The Device Work Center can be used to configure Cisco AppNav when a user has a single or few devices. You can individually edit the configurations that are deployed using a template on the devices.

To configure the Cisco AppNav from the Device Work Center:

Step 1  Choose Inventory > Device Management > Network Devices.

Step 2  Select the device to be configured.

Step 3  On the Configuration tab in the bottom pane, and click WAN Optimization.

The Cisco AppNav configuration is divided into the following sections:

• AppNav controllers—The Controllers page shows the IP addresses of routers belonging to the same cluster as the router. You must assign one of the addresses to one of the currently selected router's interfaces. Each router's own IP address is shown in a drop-down list. The IP addresses of other routers in the same cluster are listed in a separate table.

• Cisco WAAS clusters —The Cisco WAAS Clusters page is the main Cisco AppNav page. It lists the Cisco WAAS clusters configured on the device and allows new ones to be created. To view the detailed configuration for a cluster, including the policy map, select the cluster, and click Edit.

  – In this page, cluster settings and policies can be edited. Expand individual rules by clicking the arrow in the third column. This enables the corresponding rule to be edited as well as the class maps and Cisco WAAS service node groups to be viewed, modified, and created. New rules can be added by clicking Add Policy. The order of the rules within a policy map is significant and the table allows the order to modified by dragging rows or selecting a contiguous list of rows and using the Up or Down arrows in the menu bar.

  – To create a new cluster, select Add WAAS Cluster on the Cisco WAAS Cluster Overview tab. This launches a wizard that prompts for controllers, Cisco WAAS Service Node, interception interfaces, and some general cluster parameters. After providing the necessary information, click Finish for the configuration to take effect.
The wizard creates the cluster with a default policy that works for most small installations. All the TCP flows are redirected to a single node group, with the node group being monitored for overload conditions.

### Note
Because Prime Infrastructure does not support VRFs; therefore, only one Cisco WAAS cluster can be enabled at a time.

- **Interception**—The Interception page lets the administrator select interfaces on which incoming and outgoing traffic should be redirected (subject to policies). All the WAN interfaces on the router should have Cisco WAAS enabled.

- **Advanced Settings**—The Advanced Settings folder contains pages for Cisco WAAS service node groups, class maps, and policy maps. Most of this information is also available in the Cisco WAAS Clusters page, but it is helpful to be able to view the definition of these objects directly.
  - **Cisco WAAS Node Groups**—The Cisco WAAS Node Groups page allows the existing Cisco WAAS node groups to be edited and new ones to be created.
  - **Class maps and Policy maps**—The Class Maps and Policy Maps page does the same.

### Interface Roles

The Cisco AppNav solution redirects traffic only on interfaces on which it has been explicitly enabled. Routers differ in terms of available interfaces and how they are named. Since the templates are intended to be applied to multiple devices, they refer to interface roles instead of actual interfaces.

Interface roles are logical objects that exist only in Prime Infrastructure. They can be used in templates instead of actual interface names. When a template is deployed to a device, the interface role is resolved to a set of actual interfaces.

You can override, the set of interfaces on which Cisco WAAS is enabled during template deployment on a per-device basis. However, we recommend that you define one or more interface roles and save them as part of the template to simplify the template deployment process.

You can define interface roles in **Configuration > Templates > Shared Policy Objects > Interface Role**. For more information, see the Creating Interface Roles.

### Configuring Cisco AppNav Using Templates

Prime Infrastructure templates contain reusable chunks of configuration that can be deployed to any number of devices. WAN Optimization templates define a policy and other information that can be applied across AppNav routers.

Templates are defined in design view and can later be deployed to one or more devices. As part of the deployment process, you can fill in the device-specific parameters and preview the final CLIs before the configuration is pushed to the device. When a template is modified, it is necessary to re- to devices for the changes to take effect.

This method of configuring Cisco AppNav is used when a user needs similar Cisco AppNav configurations on multiple devices. A single template, with similar configurations, and some minor customized values can be deployed to multiple devices at the same type using the deploy option.

To configure the Cisco AppNav using templates:

#### Step 1
Choose **Configuration > Templates > Features & Technologies > WAN Optimization**.
Step 2  Select an **AppNav Cluster**.

Step 3  Enter the configuration details on the following tabs:

- Controller IP addresses—A list of controllers can be configured here or during deployment. For example, if the template is used for multiple sites, such as branches, this field must be left empty. However, values can be provided during deployment.

- Service nodes—The Cisco WAAS service node groups are used by the policy map. By default, there is a single service node group called WNG-Default. If the template is used for multiple sites, leave the service node groups empty and add the actual IP addresses during deployment. Enter the following details:
  - Name of the Service Node
  - Description
  - IP address of the Cisco WAAS Service Node

- Interception—Interface roles for which Cisco WAAS should be enabled. During deployment, an actual list of interfaces is presented. You can make a selection of the actual interfaces belonging to the device, for each device. The purpose of the interface roles is to initialize the selection with a default. Therefore, the list of enabled interface roles can be left empty in the template design view. Here you can do the following:
  - Select or unselect the **Enable WAAS** check box.

- General—A valid cluster ID range is between 1 to 32. Select the check box to enable or disable a cluster. Enter the following details:
  - Cluster ID
  - Authentication Key
  - After this, select or unselect or uncheck the **Enable Distribution** check box.

- Traffic redirection—This is a policy-related configuration, policy-map, class-maps and their relationships with ISR-WAAS groups. A simple setting results in a default policy that redirects all the TCP traffic to one node group. Select the **expert mode** to create custom policies and to redirect different types of TCP traffic to a different ISR-WAAS.

Step 4  Click **Save as Template**.

Step 5  Click **Finish**.

You can view the configured template by choosing **Configuration > Templates > Features & Technologies > My Templates**.

---

**Deploying a Cisco AppNav Template**

After a Cisco AppNav template is created, you can apply the template to begin traffic distribution.

To deploy a Cisco AppNav template:

**Step 1**  Choose **Configuration > Templates > Features and Technologies**.

**Step 2**  Select the **My Templates** folder in the left window pane.

**Step 3**  Select the Cisco WAAS template to be deployed and click **Deploy**.

You can choose a single device or multiple devices and change the required configurations.
Step 4 In the Value Assignment panel select each target device, one at a time and complete all the fields for that router:

- Basic Parameters—Includes an indication about whether the cluster is enabled.
- Controllers—The list of controller IP addresses. This must include an IP address assigned to the device itself.
- Node Groups—Enter IP addresses belonging to each of the ISR-WAAS groups used in the policy.
- Interception—A set of WAN interfaces on which Cisco WAAS interception is enabled.

Step 5 Click **Apply**.

Step 6 Click **OK**.

The Cisco AppNav is deployed on multiple devices.

---

**Note**

When a template is deployed to one or more devices, a job is created. Choose Administration > Dashboards > Job Dashboard, to verify the status of the template deployment and to view detailed status information about failures, success, or warnings. After you create a template, it can be edited multiple times depending on the requirements.

---

**Configuring Cisco AppNav Automatically During ISR-WAAS Container Activation**

This method of configuring Cisco AppNav is available only on Cisco 4451-X ISR devices or platform. Also, the software version required for ISR-WAAS activation must be Version 3.10 or later. In this method, the configuration occurs automatically as part of the installation of the Cisco WAAS virtual appliance node, ISR4451X-WAAS.

- A single service node group contains the new ISR-WAAS is created.
- Class maps are created for different types of traffic optimized by the Cisco WAAS service node.
- A default policy map, that redirects all TCP traffic to the Cisco WAAS service node, is generated.
- A Cisco WAAS cluster is created.
- Cisco WAAS is enabled on interfaces denoted by an interface role (specified at the time of container activation).

For more information on how to configure Cisco AppNav using this method, see the Installing an ISR-WAAS Container.
Configuring the Cisco WAAS Container

The Cisco Wide Area Application Services (Cisco WAAS) container is a powerful WAN optimization acceleration solution.

- Prerequisites for Installing an ISR-WAAS Container
- Installing an ISR-WAAS Container on a Single Router
- Installing an ISR-WAAS Container on Multiple Routers
- Uninstalling a Single Cisco ISR-WAAS Container
- Deactivating a Cisco ISR-WAAS Container

Note

In this chapter, ISR-WAAS device refers to the router and ISR-WAAS container refers to the container.

Prerequisites for Installing an ISR-WAAS Container

Before you install a Cisco WAAS container, you must configure the following in Cisco Prime Infrastructure:

- Cisco WAAS Central Manager Integration
- Interface Roles
- Importing an OVA image

Note

Ensure that the name of the ISR-WAAS container does not exceed 22 characters.

Cisco WAAS Central Manager Integration

To manage the ISR-WAAS with the Cisco WAAS Central Manager, you must register with the Cisco WAAS Central Manager. Registration of ISR-WAAS with Cisco WAAS Central Manager can be done either from the ISR-WAAS CLI, or from the Cisco WAAS Central Manager GUI, or while activating the ISR-WAAS through Prime Infrastructure. The WCM periodically polls the Cisco 4451-X Integrated Services Router (ISR) to retrieve the current status information and perform configuration synchronization.

Text Part Number:
Cisco WAAS Central Manager Integration

A typical Cisco WAAS deployment consists of both Prime Infrastructure and Cisco WAAS Central Manager applications. Cisco WAAS Central Manager IP is used during ISR-WAAS activation. After ISR-WAAS is activated, it registers with Cisco WAAS Central Manager. Prime Infrastructure needs the IP address and the server name of WCM for the following reasons:

- To inform Cisco WAAS Central Manager of the new Cisco ISR-WAAS
- For cross-launching Cisco WAAS Central Manager GUI for monitoring purposes

---

**Note**

Cisco WAAS Central Manager configuration is a one-time configuration. The Cisco WAAS Central Manager IP address is required for Prime Infrastructure to authenticate itself to Cisco WAAS Central Manager, and is configured in Prime Infrastructure using the Settings menu.

---

**Note**

If Cisco WAAS Central Manager IP is not configured in Prime Infrastructure, the newly activated ISR-WAAS will not be registered with Cisco WAAS Central Manager.

---

To configure the Cisco WAAS Central Manager IP address and server name in Prime Infrastructure:

**Step 1** Choose Administration > Settings > System Settings.

**Step 2** Click Service Container Management.

**Step 3** Enter the WCM IP address and the WCM server name.

**Step 4** Click Save.

WCM can be deployed under the following condition:

Prime Infrastructure works only with the active Cisco WAAS Central Manager that is configured in Prime Infrastructure.

After a Cisco WAAS Central Manager failover, one of the following must take place for Prime Infrastructure-Cisco WAAS Central Manager interworking to operate properly again:

- Prime Infrastructure is reconfigured with the IP address of the new Cisco WAAS Central Manager.
- The failed Cisco WAAS Central Manager must become active.

---

Configuring Single Sign-On

Configuring the Single Sign-On (SSO) feature provides a seamless method to launch Cisco WAAS Central Manager from Prime Infrastructure using the existing Single Sign-On functionality.

To configure SSO:

**Step 1** Choose Administration > User, Roles & AAA > SSO Servers.

**Step 2** Choose Add SSO Server from the Select a command drop-down list.

**Step 3** Select the type of SSL/TLS certificate being used by the SSO server. Select from either Self-Signed Certificate or Certificate Authority (CA) certificate type.
Step 4  If using Self-Signed Certificate type enter the IP address of the Prime Infrastructure acting as the SSO server. If using CA certificate enter either the IP address or the FQDN of the server of the Prime Infrastructure server that will be the SSO server.

Note  The browser cookies that provide the Single Sign-On functionality are stored in the browser according to either the IP address or the FQDN given here. So, you must be consistent in entering either the IP address or the FQDN across all of the clients to the SSO server.

Step 5  Click GO.

Step 6  Click Save.

Step 7  Select AAA Mode Settings.

Step 8  Select the SSO radio button.

Step 9  Click Save.

Step 10  Configure the WCM IP address. For information on how to configure the WCM IP address, see the Cisco WAAS Central Manager Integration.

Step 11  After you configure the IP address, log out of Prime Infrastructure and log in to WCM and create a username.

Creating a Username in Cisco WAAS Central Manager

Step 1  Log in to WCM.

Step 2  Choose Home > Admin > AAA > Users.

Step 3  Click Create.

Step 4  Enter a username that matches the Prime Infrastructure username.

Step 5  Choose Role Management and click admin to assign a RBAC role to create a user account.

Step 6  Choose Domain Management and assign a role and domain.

Step 7  Click Submit.

Step 8  Choose Devices > Configure > AAA > NCS Single Sign-On.

Step 9  Select the Enable NCS Single Sign-On check box and enter the CAS/SSO server URL.

Step 10  Click Submit to create the certificate.

Step 11  Click Submit after the certificate is created.

Cross-Launching Cisco WAAS Central Manager

You can cross-launch Cisco WAAS Central Manager in the following ways:

• Cross-Launching Cisco WAAS Central Manager on a Single Device
• Cross-Launching Cisco WAAS Central Manager on Multiple Devices
Cross-Launching Cisco WAAS Central Manager on a Single Device

To cross-launch the Cisco WAAS Central Manager from the Device Work Center:

**Step 1** Choose **Inventory > Device Management > Network Devices**.

**Step 2** Select the ISR-WAAS device.

The device details are displayed in the pane below.

**Step 3** Click the **Service Container** tab.

**Step 4** Select the corresponding ISR-WAAS container and click **Launch WCM**.

Cross-Launching Cisco WAAS Central Manager on Multiple Devices

To cross-launch from the Deployed Services:

**Step 1** Choose **Operate > Deployed Services**.

**Step 2** Select the corresponding ISR-WAAS container and click Launch WCM.

**Note** The Cisco ISR-WAAS Container Lifecycle enables a user to install, uninstall, activate, or deactivate the service container.

Defining Interface Roles

You can define interface roles in **Configuration > Templates > Shared Policy Objects > Interface Role**. For more information on creating interface roles, see the **Creating Interface Roles**. Policy objects enable users to define logical collections of elements. Policy Objects are reusable, named components that can be used by other objects and policies. The Shared Policy Objects also eliminate the need to define a component each time you define a policy. For more information on Shared Policy Objects, see the **Shared Policy Objects**.

Importing an OVA image

To import an OVA image for an ISR-WAAS container:

**Step 1** Choose **Services > Router Virtual Containers > WAAS-XE**.

**Step 2** Select an OVA image from one of the following locations:

- Device
- URL
- Protocol
• File

Step 3 Click Submit to import the image into Prime Infrastructure.

Step 4 Click Refresh to view the imported image in the Services > Router Virtual Containers > WAAS-XE > Services Catalogue folder.

### Configuring Cisco AppNav Automatically During ISR-WAAS Container Activation

A Cisco WAAS container can be configured in two different ways depending on whether you want to configure it on a single router (Installing an ISR-WAAS Container on a Single Router) or multiple routers (Installing an ISR-WAAS Container on Multiple Routers).

Installation of the ISR-WAAS container can be done in two ways. You can either install the container and activate it later, or you can install and activate the container at the same instance.

**Note** Ensure that the name of the ISR-WAAS container does not exceed 22 characters.

### Installing an ISR-WAAS Container

To install an ISR-WAAS container:

**Step 1** Choose Services > Router Virtual Containers > WAAS-XE > Services Catalogue to import an OVA image. For information on how to import an OVA image, see the Defining Interface Roles.

**Step 2** After importing, click Refresh to view the imported image.

**Step 3** Click Deploy.

**Step 4** In the Network Wizard page, select the ISR-WAAS device on which you want to configure the container.

**Step 5** Choose the Install option and select a Resource Profile from the drop-down list.

**Step 6** Click OK to install the ISR-WAAS container.

**Note** To successfully install and activate an ISR-WAAS, you need to have enough memory for each resource profile. For ISR-WAAS-750, you need 4194304 KB memory and two CPUs, for ISR-WAAS-1300, you need 6291456 KB memory and four CPUs, and for ISR-WAAS-2500, you need 8388608 KB memory with six CPUs.

### Installing and Activating an ISR-WAAS Container

To install and activate a ISR-WAAS container:

**Step 1** Choose Services > Router Virtual Containers > WAAS-XE > Services Catalogue to import an OVA image. For information on how to import an OVA image, see the Defining Interface Roles.
Installing an ISR-WAAS Container on a Single Router

To install an ISR-WAAS container on a single router:

Step 1  Choose Inventory > Device Management > Network Devices.
Step 2  From the list that is displayed, choose the router on which you want to install the ISR-WAAS container.
Step 3  Click the Service Container tab.
Step 4  Click Add and enter the configuration details in each field.
Step 5  Click OK.

Installing an ISR-WAAS Container on Multiple Routers

To install an ISR-WAAS container on multiple routers:

Step 1  Choose Services > Router Virtual Containers.
Step 2  Select the ISR-WAAS folder that contains the imported OVA image.
Step 3  Click Deploy.
   From the list that is displayed, select the routers on which you want to install the ISR-WAAS container.
   After you deploy, you can either click Install (Installing an ISR-WAAS Container) or Install and Activate (Installing and Activating an ISR-WAAS Container)
Step 4  If you choose Install and Activate, enter the following details in the Value Assignment area:
   - Enter the ISR-WAAS IP Address/Mask
Uninstalling and Deactivating a Cisco WAAS Container

You can deactivate a Cisco WAAS Container either from the Device Work Center or from the Deployed Services. From the Device Work Center, you can deactivate a single ISR-WAAS container, but from the Deployed Services, you can deactivate multiple ISR-WAAS containers.

Uninstalling a Single Cisco ISR-WAAS Container

To uninstall a single ISR-WAAS container from the Device Work Center:

Step 1. Choose Inventory > Device Management > Network Devices.
Step 2. From the list that is displayed, select the router from which you want to uninstall the Cisco WAAS container by clicking it.
Step 3. Click the Service Container tab in the bottom pane.
Step 4. Click Uninstall.
Step 5. Click OK.

Uninstalling a Multiple Cisco ISR-WAAS Container

To uninstall multiple Cisco ISR-WAAS containers from the Deployed Services:

Step 1. Choose Services > Router Virtual Containers > WAAS-XE > Deployed Services.
Step 2. From the list that is displayed, select the routers from which you want to uninstall the Cisco WAAS containers by clicking them.
Step 3. Click Uninstall.
Step 4. Click OK.

Note

When a Cisco WAAS virtual appliance is uninstalled through Prime Infrastructure, the corresponding Cisco AppNav configuration is removed.
Deactivating a Cisco ISR-WAAS Container

You can deactivate a Cisco ISR-WAAS container in the following two ways:

- Deactivating a Single Cisco ISR-WAAS Container
- Deactivating Multiple Cisco ISR-WAAS Containers

Deactivating a Single Cisco ISR-WAAS Container

To deactivate a single Cisco ISR-WAAS container from the Device Work Center:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Inventory &gt; Device Management &gt; Network Devices.</td>
</tr>
<tr>
<td>2</td>
<td>Select a Cisco ISR-WAAS device name from the device group list.</td>
</tr>
<tr>
<td>3</td>
<td>Click the Service Container tab.</td>
</tr>
<tr>
<td>4</td>
<td>Click Deactivate.</td>
</tr>
</tbody>
</table>

Deactivating Multiple Cisco ISR-WAAS Containers

To deactivate multiple Cisco WAAS containers from the Deployed Services:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Services &gt; Router Virtual Containers &gt; WAAS-XE &gt; Deployed Services.</td>
</tr>
<tr>
<td>2</td>
<td>Choose multiple ISR-WAAS device names from the list.</td>
</tr>
<tr>
<td>3</td>
<td>Click Deactivate.</td>
</tr>
</tbody>
</table>
Working with Wireless Mobility

- What Is Mobility?
- New Mobility
- Mobility Work Center
- Creating a Mobility Domain
- Mobility Anchors

What Is Mobility?

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another securely and with as little latency as possible. To allow more flexible roaming and to minimize the need for tunnel encapsulation of traffic, Cisco Prime Infrastructure provides a robust mobility architecture that distributes mobility functionality across the network devices.

The following are the key elements of the mobility architecture:

- Mobility Controller (MC)—The MC (for example, Cisco 5700 Series Wireless Controller) is responsible for one or more MAs or switch peer groups, handling roaming within its span of control, and transiting traffic between MAs and/or MCs when co-located with MTE.
- Mobility Agent (MA)—The MA (for example, Catalyst 3650 or Catalyst 3850 Switch) resides in the access switch or edge switch that the WAP is directly connected to, and terminates at the CAPWAP tunnel for communications with the WAP.
- Mobility Oracle (MO)—The MO is a top-level control entity responsible for connecting multiple MCs or mobility subdomains in deployments of the largest scale, to enable roaming across very large physical areas.
- Mobility Domain—A roaming domain: a mobile user may roam across all of the devices in this domain (the set of WAPs and all of the control entities associated with it). This typically includes MAs and MCs, and may include a MO (to join multiple subdomains).
- Mobility Sub-Domain—The set of WAPs and associated MAs and one MC, representing a portion of a larger mobility domain (where a MO serves to coordinate roaming between multiple sub-domains).
- Switch Peer Group (SPG)—A group of switches (acting as MAs). An SPG establishes a full mesh of mobility tunnels among the group members to support efficient roaming across the WAPs associated with the switches in the group. An SPG is also intended to limit the scope of interactions between switches during handoffs. An SPG is configured by the Mobility Controller, and every switch in the switch peer group has the same view of the membership. The switches in an SPG might
be interconnected by a set of direct tunnels. When a station roams from one switch to another within the same switch peer group, if the point of presence stays at the original or anchor switch, the traffic can be directly tunneled back to the anchor switch without involving the MTE. This direct tunneling mechanism is a data path optimization and is optional.

- **Mobility Group**—A mobility group is a set of MCs (and their associated MAs / switch peer groups)
- **Mobility Tunnel Endpoint**—The Mobility Tunnel Endpoint (MTE) provides data plane services for mobile devices through the use of tunneling. This minimizes the impact of roaming events on the network by keeping the user’s point of presence on the network a constant. If the VLAN or subnet of the roamed client is available at the MTE, the MTE could become the point of presence; otherwise it merely functions as a tunnel switching entity that connects the roamed client to access switch or MTE that is the point of presence.

**Related Topics**
- Mobility Work Center
- Creating a Mobility Domain

### New Mobility

**Hierarchical Mobility** is referred to as New Mobility in the wireless LAN controller configuration. Prime Infrastructure 2.0 supports the new mobility functionality for Cisco 5508 and WiSM2 platforms that run Cisco WLC 7.6.

The key features of the New Mobility functionality in Prime Infrastructure are:

- **Mobility Work Center** discovers Cisco 5508 and WiSM 2 platforms that run Cisco WLC 7.6 and provide necessary operations related to building hierarchical mobility architecture that involves two device types (Cisco 5508 and WiSM2) and Cisco 3650/3850 deployed as Mobility Agent.
- When deploying the hierarchical mobility architecture, the wireless features such as WLAN, VLAN, security, guest anchor can be configured on Cisco 5508 and WiSM2 using the LifeCycle view.
- Deploying the flat mobility architecture on Cisco 5508 and WiSM2 would be supported only in classic view and entire wireless configuration would be left as it is in classic and LifeCycle view.
- As in Prime Infrastructure 2.O, the IOS based devices 3850 and 5760 continue to be configured using CLI templates for some of the wireless features such as creating VLAN interfaces.

For more information about the new mobility functionality, see the Hierarchical Mobility (New Mobility) the Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.3.112.0 Release Notes at:
http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn7_3_112_0.html#wp1054557

### Mobility Work Center

The Mobility Work Center is available by choosing **Services > Mobility Services > Mobility Domains**. The following information is displayed:

- **Device Name**—Name of the MC.
- **Management IP**—Management IP address of the MC.
- **Wireless Interface IP**—IP address on the MC which is used for mobility protocol.
• Mobility Group—Name of the mobility group the MC belongs to.
• Mobility Role—Shows administrative and operational mobility mode. If Admin and Operational values are different, the device needs reboot for the administrative mode to be effective. It shows MO in addition to mobility mode if Mobility Oracle is enabled on it.

In this page, you can perform the following tasks:
• Create Mobility Domain—See Creating a Mobility Domain.
• Create Switch Peer Group—To create switch peer groups in MC.
• Change Mobility Role—To change the controllers from MA to MC.
• Delete Domain—Deletes only the domain; it does not delete the controllers from Prime Infrastructure.
• Delete Members—To remove selected MCs from a selected domain.
• Set as Mobility Oracle—To enable MO on a selected MC, if the MC must act as the MO for the entire domain. There can be only one MO per domain. Only Cisco 5760 series controllers support the MO feature.
• Add members to switch peer group—To add members to switch peer group.
• Delete members from switch peer group—To delete members from switch peer group.

By default, the Mobility Work Center page displays all of the mobility domains configured in the managed network. To see a list of mobility devices, choose All Mobility Devices from the left sidebar.

Related Topics
• What Is Mobility?
• Creating a Mobility Domain

Creating a Mobility Domain

A mobility domain is a collection of controllers that have all been configured with each other’s IP addresses, allowing clients to roam between the controllers in the mobility domain.

The Mobility Work Center displays all mobility domains configured in the managed network using Prime Infrastructure. The left sidebar menu shows:
• Domains
• MCs in each domain
• SPGs on each MC
• MAs in each SPG

When a node is selected from the left sidebar, the right pane shows more details. When a domain node is selected from the left sidebar, the right pane displays the MCs in the domain.

To create a mobility domain:

**Step 1** Choose Services > Mobility Services > Mobility Domains.
**Step 2** Click on the left sidebar menu.
**Step 3** Enter a name for the mobility domain for the set of MCs that you want to group together.
Creating a Mobility Domain

If a selected MC exists in another domain, it is removed from that domain and added to the new domain.

**Step 4** Select mobility domain member devices.
A device can belong to one domain or SPG only.

**Step 5** Click **Apply**.

Creating a Switch Peer Group

An MC can have switch peer groups (SPGs), and a switch peer group can have MAs. The MAs in a managed network are listed on the Switch Peer Group page. If you create a switch peer group when you already have one, MAs are moved from the old switch peer group to the new one, and the MC wireless interface IP address is set on all of the MAs.

To create a switch peer group, follow these steps:

**Step 1** Choose **Services > Mobility Services > Mobility Domains**
**Step 2** Choose an MC from the left sidebar.
**Step 3** Click **Create Switch Peer Group**.
**Step 4** Enter a name for the switch peer group that will contain the set of MAs that you want to group together on the selected MC.
If a selected MA exists in another switch peer group, it is removed from that group and added to the new group. You can create multiple switch peer groups on an MC.
**Step 5** Select mobility agents.
A device can belong to one domain or SPG only.
**Step 6** Click **Apply**.
The SPG that you created appears in the left sidebar. You can navigate to it to see the mobility agents on the selected switch peer group.

Changing a Mobility Role

By default, Cisco 3850 controllers act as MAs. These controllers can be converted to MCs if MCs are needed in the network.

To change a mobility role:

**Step 1** Choose **Services > Mobility Services > Mobility Domains**.
**Step 2** Choose **All Mobility Devices**.
**Step 3** Select a device and the role that you want to change to:
- Change Role To Mobility Controller—Enables the mobility controller feature on the selected controller.
- Change Role To Mobility Agent—Enables the Mobility Agent feature on the selected controller. When you do this, the MC feature is disabled.
Converting MAs to MCs (and vice versa) is limited to 3850 devices. For a changed role to take effect, you must reboot the device.

- Assign Mobility Group—Allows you to enter new mobility group name for the selected device.

## Mobility Anchors

Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN. This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of a client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographic load balancing because WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

### Configuring a Guest Anchor Controller for a WLAN

The guest anchor controller is a controller dedicated to guest traffic, and is located in an unsecured network area, often called the demilitarized zone (DMZ). Other internal WLAN controllers from where the traffic originates are located in the enterprise LAN.

**Note**

The Cisco 5760 controller can be a guest anchor whereas the Catalyst 3850 switch cannot be a guest anchor but it can be a foreign controller.

You can configure a guest controller as a mobility anchor for a WLAN for load balancing.

**Before You Begin**

- Ensure that wireless devices are set up in Prime Infrastructure. For more information about setting up wireless devices, see Configuring Wireless Features.
- Ensure that the wireless devices that you want to configure as mobility anchors for a WLAN are in the same mobility domain.

To configure a guest anchor controller for a WLAN:
Configuring Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to Prime Infrastructure. This feature allows Prime Infrastructure to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose Services > Mobility Services > Spectrum Experts. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address—The MAC address of the spectrum sensor card in the laptop.
- Reachability Status—Specifies whether the Spectrum Expert is successfully running and sending information to Prime Infrastructure. The status appears as reachable or unreachable.

Adding a Spectrum Expert

To add a Spectrum Expert, follow these steps:

Step 1 Choose Services > Mobility Services > Spectrum Experts.
Step 2  From the Select a command drop-down list, choose Add Spectrum Expert. This link only appears when no spectrum experts are added. You can also access the Add Spectrum Expert page by choosing Add Spectrum Expert from the Select a command drop-down list.

Step 3  Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.

To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to Prime Infrastructure.

Viewing Spectrum Experts Summary

The Spectrum Experts page provides a table of the Spectrum Experts added to the system. The table provides the following Spectrum Expert information:

- **Hostname**—Displays the host name or IP address.
- **Active Interferers**—Indicates the current number of interferers being detected by the Spectrum Experts.
- **Alarms APs**—The number of access points seen by the Spectrum Experts that are potentially affected by detected interferers.
- **Alarms**—The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert.
- **Reachability Status**—Indicates “Reachable” in green if the Spectrum Expert is running and sending data to Prime Infrastructure. Otherwise, indicates “unreachable” in red.
- **Location**—When the Spectrum Expert is a wireless client, a link for location is available. It shows the location of the Spectrum Expert with a red box that shows the effective range.

Viewing Interferers Summary

The Interferers-SEs page displays a list of all the interferers detected over a 30-day interval. The table provides the following interferer information:

- **Interferer ID**—An identifier that is unique across different spectrum experts. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device.
- **Category**—Indicates the category of the interferer. Categories include: Bluetooth, cordless phones, microwave ovens, 802.11 FH, generic: fixed-frequency, jammers, generic: frequency-hopped, generic:continuous, and analog video.
- **Type**—Active indicates that the interferer is currently being detected by a spectrum expert. Inactive indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert saw that the interferer is no longer reachable by Prime Infrastructure.
- **Discover Time**—Indicates when the interferer was discovered.
- **Affected Channels**—Identifies affected channels.
- **Number of APs Affected**—The number of access points managed by Prime Infrastructure that the spectrum expert detects or the interferers that the spectrum expert detected on the channels of the access point. Only active interferers are shown. If all of the following conditions are met, the access point is labelled as affected:
  - If the access point is managed by Prime Infrastructure.
  - If the spectrum expects detects the access point.
Creating wIPS Profiles

Prime Infrastructure provides several predefined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile ‘as is’ or customize it to better meet your needs.

Predefined profiles include:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshows
- Warehouse

The wIPS Profiles > Profile List page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles. The Profile List provides the following information for each profile:
Creating wIPS Profiles

- **Profile Name**—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.
  
  Hover your mouse cursor over the profile name to view the Profile ID and version.

- **MSE(s) Applied To**—Indicates the number of mobility services engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.

- **Controller(s) Applied To**—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

To create a wIPS profile, follow these steps:

**Step 1** Choose **Services > Mobility Services > wIPS Profiles**.

**Step 2** From the **Select a command** drop-down list, choose **Add Profile**, then click **Go**.

**Step 3** Enter a profile name in the Profile Name text box of the Profile Parameters page.

**Step 4** Select the applicable predefined profile, or choose **Default** from the drop-down list.

**Step 5** Choose **Save > Next**.

When you select **Save**, the profile is saved to the Prime Infrastructure database with no changes and no mobility services engine or controller assignments. The profile appears in the profile list.

**Step 6** To edit and delete current groups or add a new group:

a. From the **Select a command** drop-down list on the SSID Group List page, choose **Add Group** or **Add Groups from Global List**, then click **Go**.

b. Enter the group name and one or more SSID groups, then click **Save**.

**Step 7** To determine which policies are included in the current profile, choose **Profile Configuration**. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. Using this page, you can:

- Enable or disable an entire branch or an individual policy by selecting or unselecting the check box for the applicable branch or policy.
  
  By default, all policies are selected.

- Click an individual policy to display the policy description. Use the Policy Rules page add, edit, delete, and reorder the current policy rule settings.

  **Note** There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

  **Note** If the profile is already applied to a controller, it cannot be deleted.

- Configure the following settings:
  
  - **Threshold** (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues. Threshold options vary based on the selected policy.
Creating wIPS Profiles

When the threshold is reached for a policy, an alarm is triggered. Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page; choose **Monitor > Security** to access this page. The wIPS attacks are located in the Threats and Attacks section.

- **Severity**—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.
- **Notification**—Indicates the type of notification associated with the threshold.
- **ACL/SSID Group**—Indicates the ACL or SSID Group(s) to which this threshold is be applied.

**Note**

Only selected groups trigger the policy.

**Step 8**

When the profile configuration is complete, select **Next** to proceed to the MSE/Controller(s) page.

**Step 9**

In the Apply Profile page, select the mobility services engine and controller(s) to which you want to apply the current profile, then click **Apply** to apply the current profile to the selected mobility services engine/controller(s).

You can also apply a profile directly from the profile list. From the Profile List page, select the profile that you want to apply and click **Apply Profile** from the **Select a command** drop-down list. Then click **Go** to access the Apply Profile page.
Managing Reports

Cisco Prime Infrastructure reporting is necessary to monitor the system and network health as well as troubleshoot network problems. A number of reports can be generated to run on an immediate or a scheduled basis. Reports can also be combined to form composite reports. Each report type has a number of user-defined criteria to aid in defining the reports. The reports can be formatted as a summary, tabular, or combined (tabular and graphical) layout. After they have been defined, the reports can be saved for future diagnostic use or scheduled to run on a regular basis.

Reports are saved in these formats:

- CSV: The standard format. Whenever any CSV report exceeds 15,000 records, Prime Infrastructure creates a ZIP file and stores all the CSV files for that report in the ZIP file.
- PDF: These reports are either saved to a file on Prime Infrastructure to be downloaded later or emailed to a specific email address.

Report categories are:

- Current—Provides a snapshot of data that is not time-dependent.
- Historical—Retrieves data from the device periodically and stores it in the Prime Infrastructure database.
- Trend—Generates a report using aggregated data. Data can be periodically collected from devices and a schedule can be established for report generation.
- Top N—Generates reports based on top utilization.

With Prime Infrastructure, you also have the ability to export any report that you can view, sort reports into logical groups, and archive for long-term storage.

The Reports menu provides access to all Prime Infrastructure reports as well as currently saved and scheduled reports, which includes:

- Report Launch Pad—The hub for all Prime Infrastructure reports. From this page, you can access specific types of reports and create new reports.
- Scheduled Run Results—Allows you to access and manage all currently scheduled runs in Prime Infrastructure, and to access and manage on-demand exports as well as emailed reports.
- Saved Report Templates—Allows you to access and manage all currently saved report templates in Prime Infrastructure.

For information about the report field descriptions, See “Field Reference for Cisco Prime Infrastructure Reports” in Related Topics.

Related Topics
- Generating Reports
Generating Reports

The Report Launch Pad provides access to all Prime Infrastructure reports from a single page. You can create and save new reports, view current reports, open specific types of reports, schedule a report to run later, customize the results of a report, and combine multiple reports into one single report.

To see more report details, hover the cursor over the tool tip next to the report type.

Related Topics
- Managing Reports
- Creating, Scheduling, and Running a New Report
- Combining Reports
- Customizing Report Results
- About Scheduled Reports
- About Saved Report Templates
- Prime Infrastructure Report Data Retention Periods

Creating, Scheduling, and Running a New Report

To create, schedule, and run a new report:

Step 1 Choose Reports > Report Launch Pad.

Step 2 Choose a category from the left sidebar menu to see the report types for each report category, click New corresponding to the appropriate report in the main area of the Report Launch Pad.

Step 3 In the Report Details page, complete the fields as described in the Report Launch Pad > Report Type > New section. See “Field Reference for Cisco Prime Infrastructure Reports” in Related topics. The parameters shown in the Report Details will vary with the report type. With some reports, you will need to customize the report results.

Step 4 If you plan to run this report later or as a recurring report, enter Schedule parameters as described in the Report Launch Pad > Report Type > New section. See “Field Reference for Cisco Prime Infrastructure Reports” in Related topics.

Step 5 To run the report, choose one of the following options:
- Run—Click to run the report without saving the report setup.

Note By default, the ‘Run’ button is disabled in the Unique Clients and Users Summary report. You can schedule this report to run during low utilization hours of Prime Infrastructure.
• Save—Click to save this report setup without immediately running the report. If you have entered Schedule parameters, the report runs automatically at the scheduled date and time.

• Run and Save—Click to save this report setup and run the report immediately.

**Note** By default, the ‘Run and Save’ button is disabled in the Unique Clients and Users Summary report. You can schedule this report to run during low utilization hours of Prime Infrastructure.

• Save and Export—Click to save the report, run it, and export the results to a file. You will be prompted to:
  - Select the file format (CSV or PDF) of the exported report.
  - Choose whether to send an email when the report has been generated. If you choose this option, you must enter the destination email address and the email subject line content, and choose whether you want the exported file included as an attachment to the email.
  - Click **OK**.

If the CSV file fails to open correctly, make sure you specify a comma as the List Separator in one of the following locations:
  - Control Panel > Region/Language/Region and Language > Formats > Additional Settings
  - In Excel: File > Options > Advanced > Use System Separators.

• Save and Email—Click to save the report, run it, export the results as a file, and email the file. You will be prompted to:
  - Select the exported report file format.
  - Enter the destination email address and the email subject line content
  - Click **OK**.

• Cancel—Click to return to the previous page without running or saving this report.

**Step 6** Choose **Administration > Dashboards > Job Dashboard > User Jobs.**

**Step 7** Click **Report Status** to view the status of the job.

**Step 8** Click the report name to view the last five job instances. However, you will not be able to perform any actions available under **Edit** and **Job Series** drop-down lists.

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad.

You cannot change or update generated reports for all subdomains at the same time. You can open and change the reports individually through their respective subdomains. To update all reports, delete the reports created on subdomains and regenerate virtual domain reports with the changes.

If you upgrade the Prime Infrastructure server to a higher version, you must delete and recreate the reports that were already modified and saved in the older version.

**Related Topics**

- Field Reference for Cisco Prime Infrastructure Reports
- Combining Reports
- Customizing Report Results
Combining Reports

Two or more reports can be combined and information can be filtered based on requirements. Users can select multiple reports and combine them instead of creating special reports for different scenarios. Composite reports can be created from a pre-defined list of supported reports.

To create a new composite report:

**Step 1** Choose **Reports > Report Launch Pad**. You can create a new report in one of the following ways:
- a. From the left sidebar menu, choose **Composite > Composite Report**, and then click **New**.
- b. On the Report Launch Pad page, scroll down to view the Composite section, then click **New**.

**Step 2** In the New Custom Composite Report page, enter the report title.

**Step 3** From the **Report Category** drop-down list, choose a category.

**Step 4** Select the required reports from the available list and add them to the **Selected Reports** text box. You can also remove the selected reports.

**Step 5** Choose the appropriate **Report By** category from the drop-down list. The categories differ for each report.

**Step 6** The **Report Criteria** field allows you to sort your results depending on the previous **Report By** selection made. Click **Edit** to open the Filter Criteria page and select the required filter criteria.

**Step 7** If you plan to run this report later or as a recurring report, enter the Schedule parameters given in the **Schedule** section.

**Step 8** To run the report, choose one of the following options:
- Run—Click to run the report without saving the report setup.
- Save—Click to save the report setup without immediately running the report. If you have entered the Schedule parameters, the report runs at the scheduled date and time.
- Run and Save—Click to save the report setup and run the report immediately.
- Save and Export—Click to save the report, run it, and export the results to a file or as an email attachment. For this you need to:
  - Choose the exported report file format (CSV or PDF).
  - Check the first check box if you want to send an email when the report has been generated. You must enter the destination email address and email subject line content.
  - Check the second check box if you want the exported file to be included as an attachment in the email.
  Click **OK**.
- Save and Email—Click to save the report, run it, export the results as a file, and email the file. You will be prompted to:
  - Choose the exported report file format.
  - Enter the destination email address and email subject line content.
  Click **OK**.
- Cancel—Click to return to the previous page without running or saving the report.

You can access the saved composite reports from the Saved Reports Template.
Customizing Report Results

Many reports allow you to customize their results, so that you can include / exclude the information you need. If the report you are creating permits this, it will display a Customize button. You can click this button to access the Create Custom Report page and customize the report results.

Customizing report results is sometimes required. For example, adding Flexible NetFlow (FNF) Extension parameters to the Traffic Analysis, Application, or Voice Video Data monitoring template makes those parameters part of your Prime Infrastructure monitoring setup. However, this does not mean that the collected FNF extension monitoring data will automatically appear in the corresponding Conversations reports for Core, Application Response Time (ART), and RTP performance. To ensure that FNF data is included in Conversations reports, you must add the FNF parameters to the “Data fields to include” column using the Create Custom Report page. See the Customizing page in “Field Reference for Cisco Prime Infrastructure Reports” in Related topics.

To customize report results:

2. Click the Report Title link for the appropriate report.
3. In the Report Details page, click Customize.
4. On the Create Custom Report page, complete the required information, then click Apply to confirm the changes.

The changes made in the Create Custom Report page are not saved until you click Save in the Report Details page.

About Scheduled Reports

To view all scheduled reports in Prime Infrastructure, choose Reports > Scheduled Run Results.

The scheduled report tasks are not visible outside the Virtual Domain they run in. The results of the scheduled report tasks are visible in the Reports Run Results page of the respective domains.

The list of scheduled runs can be sorted by report category, report type, time frame, and report generation method. For information about the fields on this page, see the Scheduled Run Results page in “Field Reference for Cisco Prime Infrastructure Reports” in Related topics.
About Saved Report Templates

Saved report templates are available at Reports > Saved Report Templates. From the Saved Report Templates page, you can create report templates and manage saved report templates. You can also enable, disable, delete, or run saved reports, and you can filter and sort report templates by category, type, and status. For information about the fields on the Saved Report Templates page and filtering saved report templates, see “Field Reference for Cisco Prime Infrastructure Reports” in Related topics.

The Saved Report Templates page displays the following information:

- Report Title—Identifies the user-assigned report name.
  - Click the report title to view the details for this report.
- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Virtual Domain—Identifies the name of the virtual domain under which this report is scheduled.
- Run Now—Click the run icon to immediately run the current report.

When you execute any domain based report for a sub virtual domain, the report displays all of the device attributes that are mapped to the virtual domain where you are currently logged-in.

Prime Infrastructure Report Data Retention Periods

The report shows hourly, daily or weekly data depending on the data retention period configured by choosing Administration > Settings > System Settings > Data Retention. The data is retrieved from the database based on the following conditions.
If the period is:
1. Up to last 1 day, the data is fetched from raw table.
2. From last 2 days to 4 weeks, the data is fetched from a hourly aggregated table.
3. From previous month calendar to last 12 week, the data is fetched from daily aggregated table.
4. From last 6 months to last 1 year, the data is fetched from a weekly aggregated table.

The valid range for performance data retention period is:
1. Short term Data Retain Period: 1 to 31 days.
2. Long term Data Retain Period: 2 to 756 days.
3. Medium term Data Retain Period: 7 to 365 days.
4. Hourly Data Retain Period: Valid Range: is 1 to 31 hours.
5. Daily Data Retain Period: 7 to 365 hours.
6. Weekly Data Retain Period: 2 to 108 hours.

You can edit the the maximum number of records saved, the age of the records and the estimated memory usage for each table by clicking **Advanced Settings**.

For detailed information about Prime Infrastructure reports, see “Field Reference for Cisco Prime Infrastructure Reports” in Related topics.

**Related Topics**
- Field Reference for Cisco Prime Infrastructure Reports
Prime Infrastructure User Interface Reference

Cisco Prime Infrastructure is a web-based application.
If any of your installed Cisco Prime products are not yet enabled through licensing, the menu items or options for those features are not displayed in the web interface.

- Understanding the Prime Infrastructure User Interface
- Common UI Tasks
- Search Methods

Understanding the Prime Infrastructure User Interface

When you first log in to Prime Infrastructure, an overlay window shows you the major components of the graphical interface. To view this overlay window again, click your login name at the top-right of the screen, then choose Help > Getting Started.

Toolbar

The toolbar shown in Figure 60-1 is at the top of every page:

| 1 | Click to open the menu.
| 2 | Click to go to the Prime Infrastructure product page on cisco.com.
| 3 | Type to search for data within Prime Infrastructure. You can enter any text string such as a partial or complete IP address or a username.
| 4 | Displays the number of alarms, and the color corresponds to the highest severity level alarm in your network. Click to display the alarm summary window, displaying all alarms and the number of critical, major, and minor alarms.
| 5 | Displays login name and the virtual domain to which you are assigned. Click to change your user preferences, change your password, log out, access help, and submit product feedback.

Text Part Number:
Dock Window

If you typically visit a small subsection of pages in Prime Infrastructure, the Dock window provides a quick way to navigate quickly to those pages. From any page in Prime Infrastructure, you can click the Dock icon (in the upper right corner) to quickly view:

- Links to videos relevant to the current page
- Links to pages you recently visited (up to a maximum of 15)
- Links to pages you marked as favorites (up to a maximum of 15)
- Pinned items

The Dock window stays open until you close it.

Pinning Devices to a Dock Window

If there are specific devices that you want to watch closely, you can pin the devices to the Dock window. You can have a maximum of 15 pinned items.

1. From the Device 360° view, click the Add to Doc icon. The device appears under the Pinned Items section of the Dock window.
2. Click on the device link in the Dock window from anywhere in Prime Infrastructure, and the Device 360° view appears with updated information.
3. To remove an item from the Dock window, click the Trash icon next to the item. It is removed from Pinned Items.

Filters

You can use the Filter feature to display specific information about the Prime Infrastructure interface. The Filter icon is provided wherever the data is displayed in a tabular format. The following types of filters are available:

- Quick Filter—See Performing a Quick Filter
- Advanced Filter—See Performing an Advanced Filter
- Dashboard Filter—See Using Dashboard Filters
Performing a Quick Filter

This filter allows you to narrow down the data inside a table by applying a filter to a specific table column or columns. To apply different operators, use the Advanced Filter option (see Performing an Advanced Filter).

To launch the quick filter, choose Quick Filter from the Filter drop-down list.

To clear the Quick Filter, click Filter.

Performing an Advanced Filter

This filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. For example, you can choose the filter pattern by table column names and the operator from the drop-down list. In addition, you must enter filter criteria based on the data available in the Prime Infrastructure database.

To launch advanced filtering, choose Advanced Filter from the Filter drop-down list.

To save the filter criteria used in the Advanced filter, follow these steps:

1. Enter the advanced filter criteria, then click Go. The data is filtered based on the filter criteria.
2. After the data is filtered, click the Save icon.
3. In the Save Preset Filter dialog box, enter a name for the preset filter and click Save.

Using Dashboard Filters

The Filters toolbar allows you to narrow down the data that is displayed in all of the dashlets in a dashboard. Use this toolbar to filter the dashlets data by:

- Time frame—Select one of the preset options or create a custom time frame.
- Applications—Select a service, up to 10 individual applications, or all applications.
- Network Aware—Select wired, wireless, or all networks.
- Site—Select a site, unassigned sites, or all sites.
Understanding the Prime Infrastructure User Interface

To filter the data for all dashlets in a dashboard, follow these steps:

Step 1  Open a dashboard (for example, choose Dashboard > Overview > General).
Step 2  Change the settings in any of the Filters toolbar options, then click Go.

Data Entry Features

In addition to the check boxes, drop-down lists and data entry fields common in most user interfaces, Prime Infrastructure uses some specialized data-entry features. These features are designed to keep your view of the network as uncluttered as possible, while still making it possible for you to add, update, and save your settings when needed. These specialized data-entry features include:

- Edit Tables
- Data Popups

Edit Tables

Prime Infrastructure uses tables to display many kind of data, including lists of sites, devices, and events. The data is arranged in rows and columns, much like a spreadsheet.

An edit table differs from other tables in that you can add, edit, or delete the data it contains. Some edit tables also give you access to filters (see Filters). Edit tables are often displayed in data popups that are triggered by check boxes.

To use edit tables:

- To add a new row in the edit table:
  Click the (+) icon, complete the fields in the new row, and click Save.
- To delete one or more existing rows in an edit table:
  Select the row header check box (at the extreme left of each row), then click Delete.
- To update an entry in any field in any edit table row:
Click the row header or on the field itself, edit the contents, then click **Save**.

### Data Popups

A data popup is a window associated with a check box, anchored field, or other data-entry feature. It is displayed automatically when you select a feature, so that you can view or update the data associated with that feature. In addition to containing check boxes, drop-down lists, and data-entry fields, data popups can also contain edit tables.

To use a data popup:

1. Select the feature that triggers the data popup, such as an anchored field or a check box.
2. With the associated popup displayed, view or update the fields as needed.
3. When you are finished, click anywhere outside the data popup. If you entered new information or changed existing information, your changes are saved automatically.

**Related Topics**
- **Edit Tables**

### Interactive Graphs

Prime Infrastructure provides interactive line, area, pie, and stacked bar graphs of both time-based and non time-based data. Interactive graph features include the following:

- Support for automatic refresh—The graphs refresh automatically within a predetermined time interval.
- Two graph views:
  - Graph (Chart) view (this is the default)
  - Table (Grid) view
- Graph enlargement

**Related Topics**
- **Using Interactive Graphs**
- **Time-based Graphs**

### Using Interactive Graphs

The following table summarizes how to use interactive graphs.

| **Table 60-1** Using Interactive Graphs |  |
| **To do this:** | **Do this:** |
| Get help with the graph buttons | Hover your mouse cursor over the button. Prime Infrastructure displays a popup tooltip describing the button. |
| View the data as a graph or chart. | Click **View in Chart**. |
Table 60-1  Using Interactive Graphs

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the data in grid or table form</td>
<td>Click <strong>View in Grid</strong>.</td>
</tr>
<tr>
<td>Enlarge the graph</td>
<td>Click the button located at the bottom right side of the graph. Prime Infrastructure displays an enlarged version of the graph in a separate page. The <strong>View in Chart</strong> and <strong>View in Grid</strong> toggle buttons are available in the new page, so you can change the type of enlarged graph displayed.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Interactive Graphs
- Time-based Graphs

**Time-based Graphs**

Some graphs display time-based data. For these time-based graphs, Prime Infrastructure provides a link bar at the top of the graph. The link bar contains a set of links representing standard time-frames (such as the last six hours, one day, and so on) appropriate for the type of data in the chart. When you select one of these time-frame links, the data for that time frame is retrieved and the graph is refreshed to show only the data for that time-frame.

The time-frame links displayed in time-based graphs include the following:

- **6h**—Denotes the last six hours of data from the current time. The data is gathered from the current database table.
- **1d**—Denotes the last day (24 hours) of data from the current time. The data is gathered from the current database table.
- **1w**—Denotes the last week (seven days) of data from the current time. The data is gathered from the hourly aggregated table.
- **2w**—Denotes the last two weeks of data from the current time. The data is gathered from the hourly aggregated table.
- **4w**—Denotes the last four weeks of data from the current time. The data is gathered from the hourly aggregated table.
- **3m**—Denotes the last three months of data from the current time. The data is gathered from the daily aggregated table.
- **6m**—Denotes the last six months of data from the current time. The data is gathered from the weekly aggregated table.
- **1y**—Denotes the past year (12 months) of data from the current time. The data is gathered from the weekly aggregated table.
- **Custom**—User-selected time period. You can set the day and time for the start and end dates. The use of a current or hourly, daily, or weekly aggregated source for data depends upon the selected start date.

The default, maximum and minimum retention periods for the aggregated data displayed in time-based graphs are controlled by Prime Infrastructure administrators. For details, see “About Historical Data Retention” in Related Topics.
Related Topics

- Interactive Graphs
- Using Interactive Graphs
- About Historical Data Retention

Common UI Tasks

You can perform the following actions from nearly any Prime Infrastructure window:

- Changing Your Password
- Changing Your Active Domain
- Setting Your Home Page
- Changing User Preferences
- Getting Device Details from Device 360° View
- Getting User Details from the User 360° View
- Getting VRF Details from Router 360° View

Changing Your Password

Step 1: Click your login name at the top-right of the screen and choose Change Password.
Step 2: Click the information icon to review the password policy.
Step 3: Enter a new password as directed and click Save.

Changing Your Active Domain

Step 1: Click your login name at the top-right of the screen and choose Virtual Domain.
Step 2: Choose a domain from the list of domains of which you are a member.

Setting Your Home Page

Step 1: Navigate to the page that you want to set as your home page.
Step 2: Click your login name at the top-right of the screen and choose Set Current Page as Home.
Changing User Preferences

You can modify how many items are displayed on list pages, map settings, idle timeout settings, and alarm display options.

**Step 1**
Click your login name at the top-right of the screen and choose My Preferences.

**Step 2**
Modify any of the settings, then click Save.

Getting Device Details from Device 360° View

The Device 360° View provides detailed device information including device status, interface status, and associated device information. You can see the device 360° view from nearly all pages in which device IP addresses are displayed.

To launch the 360° view of any device, click the info icon next to the device IP address.

**Figure 60-5** shows a sample of the Device 360° View.

**Note**
The features that appear in the Device 360° View differ depending on the device type.

**Figure 60-5 Sample Device 360° View**
### Table 60-2  Device 360° View Features

<table>
<thead>
<tr>
<th>Device 360° View Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device status</td>
<td>Indicates whether the device is reachable, is being managed, and is synchronized with the Prime Infrastructure database.</td>
</tr>
<tr>
<td>Action drop-down list</td>
<td>Choose one of the following options from the <strong>Action</strong> drop-down list at the top right of the device 360° view.</td>
</tr>
<tr>
<td></td>
<td>• Alarm Browser—Launches the Alarm Browser. See Monitoring Alarms for more information.</td>
</tr>
<tr>
<td></td>
<td>• Device Details—Displays device details.</td>
</tr>
<tr>
<td></td>
<td>• Support Community—Launches the Cisco Support Community. See Launching the Cisco Support Community.</td>
</tr>
<tr>
<td></td>
<td>• Support Request—Allows you to open a support case. See Opening a Support Case for more information.</td>
</tr>
<tr>
<td></td>
<td>• Ping—Allows you to ping the device.</td>
</tr>
<tr>
<td></td>
<td>• Traceroute—Allows you to perform a traceroute on the device.</td>
</tr>
<tr>
<td></td>
<td>• Connect to Device—Allows you to connect to the device using Telnet, SSH, HTTP, and HTTPS protocols.</td>
</tr>
<tr>
<td></td>
<td>• Sync Now—Allows you to synchronize the device with the configuration stored in the Prime Infrastructure database.</td>
</tr>
<tr>
<td></td>
<td>• Routing Table Info—Shows the VRF details for routers, Cisco catalyst 4500 series switches and nexus devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> There are some prerequisites for 360° view Telnet and SSH to work in client browser.</td>
</tr>
<tr>
<td></td>
<td>• Firefox: Use external applications such as Putty for Telnet, and FireSSH add-on for SSH.</td>
</tr>
<tr>
<td></td>
<td>• Internet Explorer (IE) and Google Chrome: Add Regedit entries for Telnet and SSH. (See Related Topics.)</td>
</tr>
<tr>
<td>Alarms</td>
<td>Lists alarms on the device, including the alarm status, time stamp, and category.</td>
</tr>
<tr>
<td>Modules</td>
<td>Lists the device modules and their name, type, state, and ports.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Lists the device interfaces and the top three applications for each interface. Shows the configured VRFs (only for routers, Cisco catalyst 4500 series switches and nexus devices).</td>
</tr>
<tr>
<td>Neighbors</td>
<td>Lists the device neighbors, including their index, port, duplex status, and sysname.</td>
</tr>
<tr>
<td>Civic Location</td>
<td>Lists the Network Mobility Services Protocol (NMSP) status, civic address and location details of the device.</td>
</tr>
<tr>
<td>Wireless Interfaces</td>
<td>Lists the interface names, associated WLANs, VLAN IDs and IP addresses.</td>
</tr>
<tr>
<td>WLAN</td>
<td>Lists the WLAN names, SSIDs, security policies, and number of clients.</td>
</tr>
<tr>
<td>Recent Changes</td>
<td>Lists the last five audit changes made by user on the selected device. These changes are categorized as:</td>
</tr>
<tr>
<td></td>
<td>• Inventory</td>
</tr>
<tr>
<td></td>
<td>• Configuration</td>
</tr>
<tr>
<td></td>
<td>• SWIM</td>
</tr>
</tbody>
</table>
Connecting Device using Telnet and SSH in Internet Explorer and Google Chrome

Before You Begin
Ensure that you have the Telnet and SSH browser plug-ins installed in Internet Explorer and Chrome.

Enabling Telnet client functionality in Internet Explorer

To enable Telnet client functionality in 64 bit Windows operating System with 32 bit Internet Explorer, follow these steps:

Step 1
Open the Telnet client in control panel.
- Go to Control Panel.
- Click Programs And Features.
- Click Turn Windows features on or off in the left pane.
- Check the Telnet Client check box.
- Click OK.

Step 2
Copy the 64 bit version of telnet.exe from System32 in Windows directory to SysWOW64 in the same directory.

Step 3
Add the following registry key for the 32 bit version of Internet Explorer.
- Open regedit.exe and navigate to the following registry key:
  \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL
- For backing up the key, right-click FEATURE_DISABLE_TELNET_PROTOCOL and select export. Save the key to a location where you can easily locate it when it needs to be restored.
- Right-click FEATURE_DISABLE_TELNET_PROTOCOL again and select New and select DWORD (32-bit) Value from the drop-down list.
- In the right pane, rename the New Value as iexplore.exe.
- Verify that the value for iexplore.exe is 0x00000000 and close regedit.exe.

Step 4
Copy the file System32\en-US\telnet.exe.mui to the folder SysWOW64\en-US.

Enabling SSH

Follow these steps to start SSH session in Internet Explorer.

Step 1
Create a file called ssh.reg with the following content:

REGEDIT4
[HKEY_CLASSES_ROOT\ssh]
@="URL:ssh Protocol"
"URL Protocol"=""
[HKEY_CLASSES_ROOT\ssh\shell]
[HKEY_CLASSES_ROOT\ssh\shell\open]
[HKEY_CLASSES_ROOT\ssh\shell\open\command]
@=""C:\\Program Files\\putty\\putty.exe" "%1"

Step 2  Run this file to add the information to the Windows Registry.

---

**Note**  If you perform Enabling Telnet client functionality in Internet Explorer and Enabling SSH, the changes will also be reflected in your Google chrome.

**Related Topics**
- Getting Device Details from Device 360° View

## Getting User Details from the User 360° View

The User 360° View provides detailed information about an end user, including:
- End user network connection and association
- Authentication and authorization
- Possible problems with the network devices associated with the user’s network attachment
- Application-related issues
- Other issues in the broader network

To access the 360° view for a user, follow these steps:

**Step 1**  Choose **Monitor > Monitoring Tools > Clients and Users**.

**Step 2**  Click the expand icon next to a user name under the **User Name** column. You can view the User 360° View.

*Figure 60-6* shows a sample of the User 360° View.
Common UI Tasks

Figure 60-6 Sample User 360° View

Table 60-3 User 360° View Features

<table>
<thead>
<tr>
<th>User 360° View Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User information</td>
<td>Displays key information about the end user.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Displays endpoint information. This feature requires integration with an ISE server.</td>
</tr>
<tr>
<td>Connected To</td>
<td>Displays network attachment information.</td>
</tr>
<tr>
<td></td>
<td>• Network device (access switch or AP + Controller): Visible indication of existence and severity of any active alarms associated with the device</td>
</tr>
<tr>
<td></td>
<td>• Attachment port: Visible indication of existence and severity of any active alarms associated with the port</td>
</tr>
<tr>
<td>Location Session</td>
<td>Displays network session information.</td>
</tr>
<tr>
<td></td>
<td>• The location is the Prime Infrastructure hierarchy location.</td>
</tr>
<tr>
<td></td>
<td>• Access Policy (ISE Authorization Profile): Visible indication of the existence of any errors associated with authentication. This feature requires integration with an ISE server.</td>
</tr>
<tr>
<td></td>
<td>• Endpoint compliance status. This feature requires integration with an ISE server.</td>
</tr>
<tr>
<td></td>
<td>• Session start time and end time.</td>
</tr>
<tr>
<td>Alarms</td>
<td>Click the Alarms tab to view a list of alarms and statistics associated with the network session.</td>
</tr>
<tr>
<td>Applications</td>
<td>Click the Applications tab to view a list of applications and statistics associated with the network session. Session information (Netflow/NAM data, Assurance licenses) must be available.</td>
</tr>
</tbody>
</table>

Getting VRF Details from Router 360° View

The router 360° view provides the VRF details for the following routing protocols:

- BGP Routes
Search Methods

Prime Infrastructure provides the following search methods:

- Application Search—See Performing an Application Search.
- Advanced Search—See Performing an Advanced Search.
- Saved Search—See Performing a Saved Search.

You can access the search options from any page within Prime Infrastructure.

Performing an Application Search

To quickly search for data within Prime Infrastructure, you can enter any text string such as a partial or complete IP address or a username if you are searching for a client.

Step 1 Click the Search icon at the top-right of the screen.
Step 2 In the Search text box, enter a search string and click Search Prime Infrastructure.
Step 3 Click View List to view the matching devices from the Monitor or Configuration page.
Performing an Advanced Search

To perform a more specific search in Prime Infrastructure, follow these steps:

**Step 1**  Click the Search icon at the top-right of the screen.

**Step 2**  From the Search pulldown menu, select **Advanced Search**.

**Step 3**  In the Advanced Search dialog box, choose a category from the Search Category drop-down list.

**Step 4**  Choose all applicable filters or parameters for your search.

**Note**  Search parameters change depending on the category that you selected.

**Step 5**  To save this search, select the **Save Search** check box, enter a unique name for the search in the text box, and click **Go**.

**Note**  You can decide what information appears on the search results page. See the following for more information.

The Search categories include the following:

- **Access Points**—See Searching Access Points
- **Alarms**—See Searching Alarms
- **Clients**—See Searching Clients
- **Chokepoints**—See Searching Chokepoints
- **Configuration Versions**—See Searching Configuration Versions
- **Controller Licenses**—See Searching Controller Licenses
- **Controllers**—See Searching Controllers
- **Device Type**—See Searching Device Types
- **Events**—See Searching Events
- **Interferers**—See Searching Interferers
- **Jobs**—See Searching Jobs
- **Maps**—See Searching Maps
- **Rogue Client**—See Searching Rogue Clients
- **Shunned Client**—See Searching Shunned Clients
- **Switches**—See Searching Switches
- **Tags**—See Searching Tags
- **Wi-Fi TDOA Receivers**—See Searching Wi-Fi TDOA Receivers

**Searching Alarms**

You can configure the following parameters when performing an advanced search for alarms (see Table 60-4).
Searching Jobs

You can configure the following parameters when performing an advanced search for jobs (see Table 60-5).

**Table 60-5  Search Jobs Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Name</td>
<td>Type the name of the job that you want to search.</td>
</tr>
<tr>
<td>Job Type</td>
<td>Type the job type that you want to search.</td>
</tr>
<tr>
<td>Job Status</td>
<td>Choose <strong>All Status</strong>, <strong>Completed</strong>, or <strong>Scheduled</strong>.</td>
</tr>
</tbody>
</table>

For more information, see the Monitoring Jobs.

**Note** You can use wildcards such as *,? in the Job Name and Job Type text box to narrow or broaden your search.

Searching Access Points

You can configure the following parameters when performing an advanced search for access points (see Table 60-6).
### Search Access Points Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search By</td>
<td>Choose All APs, Base Radio MAC, Ethernet MAC, AP Name, AP Model, AP Location, IP Address, Device Name, Controller IP, All Unassociated APs, Floor Area, Outdoor Area, Unassigned APs, or Alarms.</td>
</tr>
<tr>
<td>Note</td>
<td>Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select Floor Area, you also must identify its campus and building. Or, if you select Alarms, you can search for access points based on the severity of the alarm.</td>
</tr>
<tr>
<td>AP Type</td>
<td>Choose All Types, LWAPP, or Autonomous.</td>
</tr>
<tr>
<td>AP Mode</td>
<td>Choose All Modes, Local, Monitor, FlexConnect, Rogue Detector, Sniffer, Bridge, or SE-Connect.</td>
</tr>
<tr>
<td>Radio Type</td>
<td>Choose All Radios, 802.11a, or 802.11b/g.</td>
</tr>
<tr>
<td>802.11n Support</td>
<td>Select this check box to search for access points with 802.11n support.</td>
</tr>
<tr>
<td>OfficeExtend AP Enabled</td>
<td>Select this check box to search for Office Extend access points.</td>
</tr>
<tr>
<td>CleanAir Support</td>
<td>Select this check box to search for access points which support CleanAir.</td>
</tr>
<tr>
<td>CleanAir Enabled</td>
<td>Select this check box to search for access points which support CleanAir and which are enabled.</td>
</tr>
<tr>
<td>Items per page</td>
<td>Configure the number of records to be displayed in the search results page.</td>
</tr>
</tbody>
</table>

### Searching Controller Licenses
You can configure the following parameters when performing an advanced search for controller licenses (see Table 60-7).

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller Name</td>
<td>Type the controller name associated with the license search.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Choose All, Plus, or Base depending on the license tier.</td>
</tr>
<tr>
<td>Type</td>
<td>Choose All, Evaluation, Extension, Grace Period, or Permanent.</td>
</tr>
<tr>
<td>% Used or Greater</td>
<td>Choose the percentage of the license use from this drop-down list. The percentages range from 0 to 100.</td>
</tr>
<tr>
<td>Items per page</td>
<td>Configure the number of records to be displayed in the search results page.</td>
</tr>
</tbody>
</table>

### Searching Controllers
You can configure the following parameters when performing an advanced search for controllers (see Table 60-8).
You can configure the following parameters when performing an advanced search for switches (see Table 60-9).

### Table 60-9  Search Switches Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for Switches by</td>
<td>Choose All Switches, IP Address, or Switch Name.</td>
</tr>
<tr>
<td>Items per page</td>
<td>Configure the number of records to be displayed in the search results page.</td>
</tr>
</tbody>
</table>

You can configure the following parameters when performing an advanced search for clients (see Table 60-10).

### Table 60-10  Search Clients Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Type</td>
<td>Choose All, Wireless Clients, or Wired Clients.</td>
</tr>
<tr>
<td>Wireless Type</td>
<td>Choose All, Lightweight or Autonomous Clients if you chose Wireless Clients from the Media Type list.</td>
</tr>
</tbody>
</table>

**Searching Switches**

Searching Clients
Searching Chokepoints

You can configure the following parameters when performing an advanced search for chokepoints (see Table 60-10).
### Table 60-11  Search Chokepoint Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search By</td>
<td>Choose MAC Address or Chokepoint Name.</td>
</tr>
</tbody>
</table>

**Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select MAC address, you must enter the specific MAC address for this search.

### Searching Events

You can configure the following parameters when performing an advanced search for events (see Table 60-12).

### Table 60-12  Search Events Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Choose All Severities, Critical, Major, Minor, Warning, Clear, or Info. Color coded.</td>
</tr>
<tr>
<td>Event Category</td>
<td>Choose All Types, Access Points, Controller, Security, Coverage Hole, Rogue AP, Adhoc Rogue, Interference, Mesh Links, Client, Mobility Service, Location Notifications, Pre Coverage Hole, or Prime Infrastructure.</td>
</tr>
<tr>
<td>Condition</td>
<td>Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list.</td>
</tr>
</tbody>
</table>

**Note** If you selected an event category, this drop-down list contains the conditions available in that category.

Search All Events Configure the number of records to be displayed in the search results page.

### Searching Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points (see Table 60-13).

### Table 60-13  Search SE-Detected Interferers Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search By</td>
<td>Choose All Interferers, Interferer ID, Interferer Category, Interferer Type, Affected Channel, Affected AP, Severity, Power, or Duty Cycle.</td>
</tr>
</tbody>
</table>

**Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Detected By Choose All Spectrum Experts or a specific spectrum expert from the drop-down list.

Detected within the last Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.

Interferer Status From this drop-down list, choose All, Active, or Inactive.

Restrict by Radio Bands/Channels Configure the search by radio bands or channels.

Items per page Configure the number of records to be displayed in the search results page.
### Searching Wi-Fi TDOA Receivers

You can configure the following parameters when performing an advanced search for Wi-Fi TDOA receivers (see Table 60-14).

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search By</td>
<td>Choose MAC Address or Wi-Fi TDOA Receivers Name.</td>
</tr>
<tr>
<td>Note</td>
<td>Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.</td>
</tr>
</tbody>
</table>

### Searching Maps

You can configure the following parameters when performing an advanced search for maps (see Table 60-15).

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for</td>
<td>Choose All Maps, Campuses, Buildings, Floor Areas, or Outdoor Areas.</td>
</tr>
<tr>
<td>Map Name</td>
<td>Search by Map Name. Enter the map name in the text box.</td>
</tr>
<tr>
<td>Items per page</td>
<td>Configure the number of records to be displayed in the search results page.</td>
</tr>
</tbody>
</table>

### Searching Rogue Clients

You can configure the following parameters when performing an advanced search for rogue clients (see Table 60-16).

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for clients by</td>
<td>Choose All Rogue Clients, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.</td>
</tr>
<tr>
<td>Search In</td>
<td>Choose MSEs or Prime Infrastructure Controllers.</td>
</tr>
<tr>
<td>Status</td>
<td>Select the check box and choose Alert, Contained, or Threat from the drop-down list to include status in the search criteria.</td>
</tr>
</tbody>
</table>

### Searching Shunned Clients

When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client.

You can configure the following parameters when performing an advanced search for shunned clients (see Table 60-17).
Table 60-17  Search Shunned Client Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search By</td>
<td>Choose All Shunned Clients, Controller, or IP Address.</td>
</tr>
</tbody>
</table>

**Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

## Searching Tags

You can configure the following parameters when performing an advanced search for tags (see Table 60-18).

Table 60-18  Search Tags Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for tags by</td>
<td>Choose All Tags, Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area.</td>
</tr>
</tbody>
</table>

**Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search In</td>
<td>Choose MSEs or Prime Infrastructure Controllers.</td>
</tr>
<tr>
<td>Last detected within</td>
<td>Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.</td>
</tr>
<tr>
<td>Tag Vendor</td>
<td>Select the check box and choose Aeroscout, G2, PanGo, or WhereNet.</td>
</tr>
<tr>
<td>Telemetry Tags only</td>
<td>Select the Telemetry Tags only check box to search tags accordingly.</td>
</tr>
<tr>
<td>Items per page</td>
<td>Configure the number of records to be displayed in the search results page.</td>
</tr>
</tbody>
</table>

## Searching Device Types

You can configure the following parameters when performing an advanced search for device type (see Table 60-19).

Table 60-19  Search Device Type Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Device Type</td>
<td>Choose All, Switches and Hubs, Wireless Controller, Unified AP, Autonomous AP, Unmanaged AP, and Routers.</td>
</tr>
<tr>
<td>Enter Device IP</td>
<td>Enter the IP address of the device selected in the Select Device Type field.</td>
</tr>
</tbody>
</table>

## Searching Configuration Versions

You can configure the following parameter when performing an advanced search for configuration versions (see Table 60-20).

Table 60-20  Search Configuration Versions Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Tag</td>
<td>Enter the tag name.</td>
</tr>
</tbody>
</table>
Performing a Saved Search

Note
Saved searches apply only to the current partition.

To access and run a previously saved search, follow these steps:

Step 1 Click the icon in the Application Search box, then click Saved Search.
Step 2 Choose a category from the Search Category drop-down list, then choose a saved search from the Saved Search List drop-down list.
Step 3 If necessary, change the current parameters for the saved search, then click Go.
# System Time Zones

This appendix lists all the available values for the system time zone.

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Location</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Libya</td>
<td>GB-Eire</td>
<td>Kwajalein</td>
</tr>
<tr>
<td>GMT</td>
<td>Australia/Lord_Howe</td>
<td>Australia/West</td>
</tr>
<tr>
<td>Australia/Sydney</td>
<td>Australia/South</td>
<td>Australia/Queensland</td>
</tr>
<tr>
<td>Australia/Yancowinna</td>
<td>Australia/Melbourne</td>
<td>Australia/Canberra</td>
</tr>
<tr>
<td>Australia/Adelaide</td>
<td>Australia/Brisbane</td>
<td>Australia/Broken_Hill</td>
</tr>
<tr>
<td>Australia/North</td>
<td>Australia/Lindeman</td>
<td>Australia/Eucla</td>
</tr>
<tr>
<td>Australia/LHI</td>
<td>Australia/Perth</td>
<td>Australia/Tasmania</td>
</tr>
<tr>
<td>Australia/NSW</td>
<td>Australia/ACT</td>
<td>Australia/Darwin</td>
</tr>
<tr>
<td>Australia/Hobart</td>
<td>Australia/Victoria</td>
<td>Australia/Currie</td>
</tr>
<tr>
<td>EST</td>
<td>Hongkong</td>
<td>CST6CDT</td>
</tr>
<tr>
<td>GMT0</td>
<td>Iran</td>
<td>Etc/GMT-7</td>
</tr>
<tr>
<td>Etc/GMT</td>
<td>Etc/GMT-5</td>
<td>Etc/GMT+9</td>
</tr>
<tr>
<td>Etc/GMT0</td>
<td>Etc/GMT+5</td>
<td>Etc/UCT</td>
</tr>
<tr>
<td>Etc/GMT-6</td>
<td>Etc/GMT+8</td>
<td>Etc/GMT+10</td>
</tr>
<tr>
<td>Etc/GMT-9</td>
<td>Etc/GMT-11</td>
<td>Etc/GMT-13</td>
</tr>
<tr>
<td>Etc/GMT+0</td>
<td>Etc/GMT-0</td>
<td>Etc/GMT-3</td>
</tr>
<tr>
<td>Etc/GMT+8</td>
<td>Etc/GMT+11</td>
<td>Etc/Universal</td>
</tr>
<tr>
<td>Etc/GMT+4</td>
<td>Etc/UTC</td>
<td>Etc/GMT+12</td>
</tr>
<tr>
<td>Etc/Zulu</td>
<td>Etc/GMT+7</td>
<td>Etc/GMT-12</td>
</tr>
<tr>
<td>Etc/Greenwich</td>
<td>Etc/GMT-2</td>
<td>Etc/GMT+1</td>
</tr>
<tr>
<td>Etc/GMT-14</td>
<td>Etc/GMT-4</td>
<td>Etc/GMT+6</td>
</tr>
<tr>
<td>Etc/GMT+2</td>
<td>Antarctica/Palmer</td>
<td>Antarctica/Rothera</td>
</tr>
<tr>
<td>Antarctica/Casey</td>
<td>Antarctica/South_Pole</td>
<td>Antarctica/Davis</td>
</tr>
<tr>
<td>Antarctica/Syowa</td>
<td>Antarctica/DumontDUrville</td>
<td>Antarctica/Mawson</td>
</tr>
<tr>
<td>Antarctica/Vostok</td>
<td>Antarctica/McMurdo</td>
<td>W-SU</td>
</tr>
<tr>
<td>Time Zone 1</td>
<td>Time Zone 2</td>
<td>Time Zone 3</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>US/Central</td>
<td>US/Aleutian</td>
<td>US/Samoa</td>
</tr>
<tr>
<td>US/Mountain</td>
<td>US/Arizona</td>
<td>US/Michigan</td>
</tr>
<tr>
<td>US/East-Indiana</td>
<td>US/Pacific</td>
<td>US/Hawaii</td>
</tr>
<tr>
<td>US/Alaska</td>
<td>US/Eastern</td>
<td>US/Indiana-Starke</td>
</tr>
<tr>
<td>Eire</td>
<td>PRC</td>
<td>UCT</td>
</tr>
<tr>
<td>Jamaica</td>
<td>Chile/EasterIsland</td>
<td>Chile/Continental</td>
</tr>
<tr>
<td>Egypt</td>
<td>Brazil/West</td>
<td>Brazil/DeNoronha</td>
</tr>
<tr>
<td>Brazil/East</td>
<td>Brazil/Acre</td>
<td>Indian/Mahe</td>
</tr>
<tr>
<td>Indian/Antananarivo</td>
<td>Indian/Kerguelen</td>
<td>Indian/Mauritius</td>
</tr>
<tr>
<td>Indian/Chagos</td>
<td>Indian/Cocos</td>
<td>Indian/Reunion</td>
</tr>
<tr>
<td>Indian/Maldives</td>
<td>Indian/Mayotte</td>
<td>Indian/Christmas</td>
</tr>
<tr>
<td>Indian/Comoro</td>
<td>EET</td>
<td>Mideast/Riyadh88</td>
</tr>
<tr>
<td>Mideast/Riyadh89</td>
<td>Mideast/Riyadh87</td>
<td>Japan</td>
</tr>
<tr>
<td>Africa/Harare</td>
<td>Africa/Mogadishu</td>
<td>Africa/Cairo</td>
</tr>
<tr>
<td>Africa/Banjul</td>
<td>Africa/Luanda</td>
<td>Africa/Addis_Ababa</td>
</tr>
<tr>
<td>Africa/Johannesburg</td>
<td>Africa/Ouagadougou</td>
<td>Africa/Lubumbashi</td>
</tr>
<tr>
<td>Africa/Windhoek</td>
<td>Africa/Bissau</td>
<td>Africa/Nouakchott</td>
</tr>
<tr>
<td>Africa/Freetown</td>
<td>Africa/Sao_Tome</td>
<td>Africa/Brazzaville</td>
</tr>
<tr>
<td>Africa/Blantyre</td>
<td>Africa/Maseru</td>
<td>Africa/Algiers</td>
</tr>
<tr>
<td>Africa/Lome</td>
<td>Africa/Asmera</td>
<td>Africa/Tunis</td>
</tr>
<tr>
<td>Africa/Porto-Novo</td>
<td>Africa/Bamako</td>
<td>Africa/El_Aaiun</td>
</tr>
<tr>
<td>Africa/Kinshasa</td>
<td>Africa/Tripoli</td>
<td>Africa/Bujumbura</td>
</tr>
<tr>
<td>Africa/Bangui</td>
<td>Africa/Conakry</td>
<td>Africa/Lusaka</td>
</tr>
<tr>
<td>Africa/Nairobi</td>
<td>Africa/Ceuta</td>
<td>Africa/Mbabane</td>
</tr>
<tr>
<td>Africa/Timbuktu</td>
<td>Africa/Accra</td>
<td>Africa/Niamey</td>
</tr>
<tr>
<td>Africa/Gaborone</td>
<td>Africa/Djibouti</td>
<td>Africa/Lagos</td>
</tr>
<tr>
<td>Africa/Maputo</td>
<td>Africa/Kigali</td>
<td>Africa/Khartoum</td>
</tr>
<tr>
<td>Africa/Abidjan</td>
<td>Africa/Dar_es_Salaam</td>
<td>Africa/Asmara</td>
</tr>
<tr>
<td>Africa/Libreville</td>
<td>Africa/Dakar</td>
<td>Africa/Malabo</td>
</tr>
<tr>
<td>Africa/Kampala</td>
<td>Africa/Casablanca</td>
<td>Africa/Ndjamena</td>
</tr>
<tr>
<td>Africa/Monrovia</td>
<td>Africa/Douala</td>
<td>MST</td>
</tr>
<tr>
<td>Singapore</td>
<td>Europe/Copenhagen</td>
<td>Europe/Bratislava</td>
</tr>
<tr>
<td>Europe/Riga</td>
<td>Europe/Jersey</td>
<td>Europe/Uzhgorod</td>
</tr>
<tr>
<td>Europe/Luxembourg</td>
<td>Europe/Athens</td>
<td>Europe/Belfast</td>
</tr>
<tr>
<td>Europe/Samara</td>
<td>Europe/San_Marino</td>
<td>Europe/Tirane</td>
</tr>
<tr>
<td>Europe/Monaco</td>
<td>Europe/Sofia</td>
<td>Europe/Stockholm</td>
</tr>
<tr>
<td>Europe/Guernsey</td>
<td>Europe/Amsterdam</td>
<td>Europe/Sarajevo</td>
</tr>
<tr>
<td>Europe/Andorra</td>
<td>Europe/Zaporozhye</td>
<td>Europe/Bucharest</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time Zone</td>
<td>Time Zone</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Europe/Dublin</td>
<td>Europe/Zagreb</td>
<td>Europe/Ljubljana</td>
</tr>
<tr>
<td>Europe/Prague</td>
<td>Europe/Moscow</td>
<td>Europe/Vatican</td>
</tr>
<tr>
<td>Europe/Kiev</td>
<td>Europe/Warsaw</td>
<td>Europe/Chisinau</td>
</tr>
<tr>
<td>Europe/Zurich</td>
<td>Europe/Malta</td>
<td>Europe/Skopje</td>
</tr>
<tr>
<td>Europe/Volgograd</td>
<td>Europe/Vaduz</td>
<td>Europe/Rome</td>
</tr>
<tr>
<td>Europe/Brussels</td>
<td>Europe/Helsinki</td>
<td>Europe/Belgrade</td>
</tr>
<tr>
<td>Europe/Istanbul</td>
<td>Europe/Budapest</td>
<td>Europe/Madrid</td>
</tr>
<tr>
<td>Europe/Mariehamnn</td>
<td>Europe/Simferopol</td>
<td>Europe/Paris</td>
</tr>
<tr>
<td>Europe/Minsk</td>
<td>Europe/Vilnius</td>
<td>Europe/Podgorica</td>
</tr>
<tr>
<td>Europe/Isle_of_Man</td>
<td>Europe/Vienna</td>
<td>Europe/Kaliningrad</td>
</tr>
<tr>
<td>Europe/Gibraltar</td>
<td>Europe/Lisbon</td>
<td>Europe/Tallinn</td>
</tr>
<tr>
<td>Europe/Oslo</td>
<td>Europe/London</td>
<td>Europe/Nicosia</td>
</tr>
<tr>
<td>Europe/Tiraspol</td>
<td>Europe/Berlin</td>
<td>Mexico/BajaSur</td>
</tr>
<tr>
<td>Mexico/BajaNorte</td>
<td>Mexico/General</td>
<td>GMT+0</td>
</tr>
<tr>
<td>WET</td>
<td>MST7MDT</td>
<td>Turkey</td>
</tr>
<tr>
<td>Factory</td>
<td>Atlantic/St_Helena</td>
<td>Atlantic/Bermuda</td>
</tr>
<tr>
<td>Atlantic/Faeroe</td>
<td>Atlantic/Madeira</td>
<td>Atlantic/Canary</td>
</tr>
<tr>
<td>Atlantic/Jan_Mayen</td>
<td>Atlantic/Reykjavik</td>
<td>Atlantic/Stanley</td>
</tr>
<tr>
<td>Atlantic/Azores</td>
<td>Atlantic/South_Georgia</td>
<td>Atlantic/Cape_Verde</td>
</tr>
<tr>
<td>Atlantic/Faroe</td>
<td>GMT-0</td>
<td>Poland</td>
</tr>
<tr>
<td>America/El_Salvador</td>
<td>America/Montreal</td>
<td>America/St_Kitts</td>
</tr>
<tr>
<td>America/Godthab</td>
<td>America/Cambridge_Bay</td>
<td>America/Glace_Bay</td>
</tr>
<tr>
<td>America/St_Thomas</td>
<td>America/Chicago</td>
<td>America/Shiprock</td>
</tr>
<tr>
<td>America/St_Barthelemy</td>
<td>America/Chihuahua</td>
<td>America/Guadeloupe</td>
</tr>
<tr>
<td>America/Miquelon</td>
<td>America/Maceio</td>
<td>America/Toronto</td>
</tr>
<tr>
<td>America/Noronha</td>
<td>America/Swift_Current</td>
<td>America/Tortola</td>
</tr>
<tr>
<td>America/Mendoza</td>
<td>America/Argentina/Mendoza</td>
<td>America/Argentina/San_Luis</td>
</tr>
<tr>
<td>America/Argentina/Buenos_Aires</td>
<td>America/Argentina/Catamarca</td>
<td>America/Argentina/Tucuman</td>
</tr>
<tr>
<td>America/Argentina/San_Juan</td>
<td>America/Argentina/La_Rioja</td>
<td>America/Argentina/Salta</td>
</tr>
<tr>
<td>America/Argentina/Cordoba</td>
<td>America/Argentina/Jujuy</td>
<td>America/Argentina/ComodRivadav</td>
</tr>
<tr>
<td>America/Argentina/Ushuaia</td>
<td>America/Argentina/Rio_Gallegos</td>
<td>America/St_Vincent</td>
</tr>
<tr>
<td>America/Boise</td>
<td>America/Regina</td>
<td>America/Thule</td>
</tr>
<tr>
<td>America/Santiago</td>
<td>America/Menominee</td>
<td>America/Coral_Harbour</td>
</tr>
<tr>
<td>America/Caracas</td>
<td>America/Aruba</td>
<td>America/Danmarkshavn</td>
</tr>
<tr>
<td>America/Jamaica</td>
<td>America/Fortaleza</td>
<td>America/Inuvik</td>
</tr>
<tr>
<td>America/Havana</td>
<td>America/Curacao</td>
<td>America/Cuiaba</td>
</tr>
<tr>
<td>America/Guatemala</td>
<td>America/Dawson</td>
<td>America/Yakutat</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time Zone</td>
<td>Time Zone</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>America/Atikokan</td>
<td>America/Nipigon</td>
<td>America/Grenada</td>
</tr>
<tr>
<td>America/Panama</td>
<td>America/Eirunepe</td>
<td>America/Phoenix</td>
</tr>
<tr>
<td>America/Belem</td>
<td>America/Goose_Bay</td>
<td>America/Sao_Paulo</td>
</tr>
<tr>
<td>America/Vancouver</td>
<td>America/Adak</td>
<td>America/Tijuana</td>
</tr>
<tr>
<td>America/Louisville</td>
<td>America/Scoresbysund</td>
<td>America/Halifax</td>
</tr>
<tr>
<td>America/Antigua</td>
<td>America/Winnipeg</td>
<td>America/Asuncion</td>
</tr>
<tr>
<td>America/Santarem</td>
<td>America/Knox_IN</td>
<td>America/Buenos_Aires</td>
</tr>
<tr>
<td>America/Catamarca</td>
<td>America/Pangnirtung</td>
<td>America/Rainy_River</td>
</tr>
<tr>
<td>America/Rankin_Inlet</td>
<td>America/Araguaina</td>
<td>America/Atka</td>
</tr>
<tr>
<td>America/Cayenne</td>
<td>America/Campo_Grande</td>
<td>America/Mazatlan</td>
</tr>
<tr>
<td>America/Porto_Velho</td>
<td>America/Anguilla</td>
<td>America/Whitehorse</td>
</tr>
<tr>
<td>America/Nassau</td>
<td>America/Hermosillo</td>
<td>America/Guyana</td>
</tr>
<tr>
<td>America/Grand_Turk</td>
<td>America/St_Lucia</td>
<td>America/Manaus</td>
</tr>
<tr>
<td>America/Blanc-Sablon</td>
<td>America/Kentucky/Monticello</td>
<td>America/Kentucky/Louisville</td>
</tr>
<tr>
<td>America/Ensenada</td>
<td>America/Anchorage</td>
<td>America/Managua</td>
</tr>
<tr>
<td>America/Costa_Rica</td>
<td>America/La_Paz</td>
<td>America/Puerto_Rico</td>
</tr>
<tr>
<td>America/Iqaluit</td>
<td>America/Virgin</td>
<td>America/Port_Acre</td>
</tr>
<tr>
<td>America/ Yellowknife</td>
<td>America/Boa_Vista</td>
<td>America/Montserrat</td>
</tr>
<tr>
<td>America/Juneau</td>
<td>America/Port-au-Prince</td>
<td>America/Recife</td>
</tr>
<tr>
<td>America/Port_of_Spain</td>
<td>America/Barbados</td>
<td>America/Bahia</td>
</tr>
<tr>
<td>America/Monterrey</td>
<td>America/Indiana/Knox</td>
<td>America/Indiana/Marengo</td>
</tr>
<tr>
<td>America/Indiana/Vincennes</td>
<td>America/Indiana/Tell_City</td>
<td>America/Indiana/Vevay</td>
</tr>
<tr>
<td>America/Indiana/Petersburg</td>
<td>America/Indiana/Indianapolis</td>
<td>America/Indiana/Winamac</td>
</tr>
<tr>
<td>America/Resolute</td>
<td>America/Cordoba</td>
<td>America/Rosario</td>
</tr>
<tr>
<td>America/Santo_Domingo</td>
<td>America/Denver</td>
<td>America/Edmonton</td>
</tr>
<tr>
<td>America/Thunder_Bay</td>
<td>America/Merida</td>
<td>America/Dawson_Creek</td>
</tr>
<tr>
<td>America/St_Johns</td>
<td>America/Cancun</td>
<td>America/Fort_Wayne</td>
</tr>
<tr>
<td>America/Dominica</td>
<td>America/Marigot</td>
<td>America/Jujuy</td>
</tr>
<tr>
<td>America/Rio_Branco</td>
<td>America/Mexico_City</td>
<td>America/Cayman</td>
</tr>
<tr>
<td>America/Indianapolis</td>
<td>America/New_York</td>
<td>America/Guayaquil</td>
</tr>
<tr>
<td>America/Lima</td>
<td>America/Los_Angeles</td>
<td>America/Martinique</td>
</tr>
<tr>
<td>America/Belize</td>
<td>America/Bogota</td>
<td>America/Paramaribo</td>
</tr>
<tr>
<td>America/Detroit</td>
<td>America/Nome</td>
<td>America/Montevideo</td>
</tr>
<tr>
<td>America/North_Dakota/New_Salem</td>
<td>America/North_Dakota/Center</td>
<td>America/Tegucigalpa</td>
</tr>
<tr>
<td>America/Moncton</td>
<td>Cuba</td>
<td>Navajo</td>
</tr>
<tr>
<td>NZ-CHAT</td>
<td>Iceland</td>
<td>Universal</td>
</tr>
<tr>
<td>Pacific/Pitcairn</td>
<td>Pacific/Kwajalein</td>
<td>Pacific/Noumea</td>
</tr>
<tr>
<td>Pacific/Samoia</td>
<td>Pacific/Enderbury</td>
<td>Pacific/Rarotonga</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time Zone</td>
<td>Time Zone</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Pacific/Pago_Pago</td>
<td>Pacific/Tarawa</td>
<td>Pacific/Fiji</td>
</tr>
<tr>
<td>Pacific/Chatham</td>
<td>Pacific/Guadalcanal</td>
<td>Pacific/Honolulu</td>
</tr>
<tr>
<td>Pacific/Palau</td>
<td>Pacific/Galapagos</td>
<td>Pacific/Kosrae</td>
</tr>
<tr>
<td>Pacific/Majuro</td>
<td>Pacific/Guam</td>
<td>Pacific/Efate</td>
</tr>
<tr>
<td>Pacific/Funaufi</td>
<td>Pacific/Wallis</td>
<td>Pacific/Nauru</td>
</tr>
<tr>
<td>Pacific/Fakaofo</td>
<td>Pacific/Easter</td>
<td>Pacific/Norfolk</td>
</tr>
<tr>
<td>Pacific/Johnston</td>
<td>Pacific/IPa</td>
<td>Pacific/Tahiti</td>
</tr>
<tr>
<td>Pacific/Port_Moresby</td>
<td>Pacific/Saipan</td>
<td>Pacific/Tongatapu</td>
</tr>
<tr>
<td>Pacific/Midway</td>
<td>Pacific/Marquesas</td>
<td>Pacific/Kiritimati</td>
</tr>
<tr>
<td>Pacific/Gambier</td>
<td>Pacific/Niue</td>
<td>Pacific/Auckland</td>
</tr>
<tr>
<td>Pacific/Ponape</td>
<td>Pacific/Apia</td>
<td>Pacific/Tahiti</td>
</tr>
<tr>
<td>Pacific/Wake</td>
<td>Israel</td>
<td>UTC</td>
</tr>
<tr>
<td>Portugal</td>
<td>ROC</td>
<td>NZ</td>
</tr>
<tr>
<td>Canada/Central</td>
<td>Canada/Yukon</td>
<td>Canada/East-Saskatchewan</td>
</tr>
<tr>
<td>Canada/Mountain</td>
<td>Canada/Atlantic</td>
<td>Canada/Pacific</td>
</tr>
<tr>
<td>Canada/Eastern</td>
<td>Canada/Newfoundland</td>
<td>Canada/Saskatchewan</td>
</tr>
<tr>
<td>PST8PDT</td>
<td>Zulu</td>
<td>CET</td>
</tr>
<tr>
<td>Arctic/Longyearbyen</td>
<td>GB</td>
<td>ROK</td>
</tr>
<tr>
<td>EST5EDT</td>
<td>Greenwich</td>
<td>Asia/Pyongyang</td>
</tr>
<tr>
<td>Asia/Vladivostok</td>
<td>Asia/Ulaanbaatar</td>
<td>Asia/Tel_Aviv</td>
</tr>
<tr>
<td>Asia/Riyadh</td>
<td>Asia/Riyadh88</td>
<td>Asia/Baku</td>
</tr>
<tr>
<td>Asia/Kuching</td>
<td>Asia/Kashgar</td>
<td>Asia/Harbin</td>
</tr>
<tr>
<td>Asia/Katmandu</td>
<td>Asia/Riyadh89</td>
<td>Asia/Aqtobe</td>
</tr>
<tr>
<td>Asia/Thimbu</td>
<td>Asia/Baghdad</td>
<td>Asia/Colombo</td>
</tr>
<tr>
<td>Asia/Tokyo</td>
<td>Asia/Aqtau</td>
<td>Asia/Taipei</td>
</tr>
<tr>
<td>Asia/Kuwait</td>
<td>Asia/Chungking</td>
<td>Asia/Jayapura</td>
</tr>
<tr>
<td>Asia/Tashkent</td>
<td>Asia/Ujung_Pandang</td>
<td>Asia/Karachi</td>
</tr>
<tr>
<td>Asia/Dhaka</td>
<td>Asia/Singapore</td>
<td>Asia/Gaza</td>
</tr>
<tr>
<td>Asia/Sakhalin</td>
<td>Asia/Kuala_Lumpur</td>
<td>Asia/Dubai</td>
</tr>
<tr>
<td>Asia/Kabul</td>
<td>Asia/Dushanbe</td>
<td>Asia/Jakarta</td>
</tr>
<tr>
<td>Asia/Novosibirsk</td>
<td>Asia/Qyzylorda</td>
<td>Asia/Dili</td>
</tr>
<tr>
<td>Asia/Shanghai</td>
<td>Asia/Irkutsk</td>
<td>Asia/Kamchatka</td>
</tr>
<tr>
<td>Asia/Urumqi</td>
<td>Asia/Aden</td>
<td>Asia/Muscat</td>
</tr>
<tr>
<td>Asia/Magadan</td>
<td>Asia/Yekaterinburg</td>
<td>Asia/Tbilisi</td>
</tr>
<tr>
<td>Asia/Brunei</td>
<td>Asia/Krasnoyarsk</td>
<td>Asia/Hong_Kong</td>
</tr>
<tr>
<td>Asia/Omsk</td>
<td>Asia/Samarkand</td>
<td>Asia/Pontianak</td>
</tr>
<tr>
<td>Asia/Saigon</td>
<td>Asia/Hovd</td>
<td>Asia/Bahrain</td>
</tr>
<tr>
<td>Asia/Phnom_Penh</td>
<td>Asia/Ashkhabad</td>
<td>Asia/Kolkata</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Time Zone</td>
<td>Time Zone</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Asia/Bishkek</td>
<td>Asia/Macao</td>
<td>Asia/Anadyr</td>
</tr>
<tr>
<td>Asia/Calcutta</td>
<td>Asia/Ulan_Bator</td>
<td>Asia/Macau</td>
</tr>
<tr>
<td>Asia/Vientiane</td>
<td>Asia/Ashgabat</td>
<td>Asia/Istanbul</td>
</tr>
<tr>
<td>Asia/Dacca</td>
<td>Asia/Damascus</td>
<td>Asia/Yakutsk</td>
</tr>
<tr>
<td>Asia/Kathmandu</td>
<td>Asia/Makassar</td>
<td>Asia/Amman</td>
</tr>
<tr>
<td>Asia/Thimphu</td>
<td>Asia/Choibalsan</td>
<td>Asia/Manila</td>
</tr>
<tr>
<td>Asia/Yerevan</td>
<td>Asia/Tehran</td>
<td>Asia/Rangoon</td>
</tr>
<tr>
<td>Asia/Qatar</td>
<td>Asia/Almaty</td>
<td>Asia/Chongqing</td>
</tr>
<tr>
<td>Asia/Oral</td>
<td>Asia/Beirut</td>
<td>Asia/Seoul</td>
</tr>
<tr>
<td>Asia/Bangkok</td>
<td>Asia/Nicosia</td>
<td>Asia/Ho_Chi_Minh</td>
</tr>
<tr>
<td>Asia/Riyadh87</td>
<td>Asia/Jerusalem</td>
<td>MET</td>
</tr>
<tr>
<td>HST</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>