



Cisco DNA Center User Guide, Release 2.3.5

First Published: 2022-12-21

Last Modified: 2024-02-20

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	New and Changed Information 1
	New and Changed Information 1

PART I	Get Started 9
---------------	----------------------

CHAPTER 2	Get Started with Cisco DNA Center 11
	Cisco DNA Center Overview 11
	Log In 11
	Complete the Quick Start Workflow 12
	User Profile Roles and Permissions 17
	Default Home Page 17
	Cisco DNA Center Journey Map 21
	View the Remote Support Authorization Dashboard 22
	Configure SSH Credentials 23
	Use Global Search 23
	Enable Localization 25
	Subscribe to Cisco DNA Center Insights 26

CHAPTER 3	Configure Telemetry 27
	Application Telemetry Overview 27
	Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry 27
	Criteria for Enabling Application Telemetry on Devices 28
	Provision Application Telemetry Settings 30
	Enable Application Telemetry for Wireless Controllers 31
	Update Telemetry Settings to Use a New Cluster Virtual IP Address 32

Update Device Configuration Using Telemetry 33

PART II

Discover and Manage Network Inventory and Topology 35

CHAPTER 4

Discover Your Network 37

Discovery Overview 37

Discovery Dashboard 38

Discovery Prerequisites 38

Discovery Credentials 39

Discovery Credentials and Cisco ISE 43

Guidelines and Limitations for Discovery Credentials 43

Discovery Credentials Example 44

Preferred Management IP Address 45

Discovery Configuration Guidelines and Limitations 45

Perform Discovery 46

Discover Your Network Using CDP 46

Discover Your Network Using an IP Address Range or CIDR 48

Discover Your Network Using LLDP 50

Manage Discovery Jobs 52

Stop and Start a Discovery Job 52

Change Credentials in a Discovery Job 52

Clone a Discovery Job 53

Delete a Discovery Job 53

CHAPTER 5

Manage Your Inventory 55

About Inventory 56

Inventory and Cisco ISE Authentication 56

Display Information About Your Inventory 57

Display Information About a Device 62

Display Information About a Device's Interface 66

Display Information About Ethernet Ports 67

Manage Port Details 69

Inventory User Interface Enhancement 70

Manage User-Defined Fields 71

Create User-Defined Fields	71
Add User-Defined Fields to a Device	72
Launch Topology Map from Inventory	72
Types of Devices in the Cisco DNA Center Inventory	72
Manage Network Devices	73
Add a Network Device	73
Update Network Device Credentials	78
Security Focus for Network Devices	82
View the Integrity Verification Status of a Device	82
Manage Compute Devices	83
Add a Compute Device	83
Update Compute Device Credentials	86
Manage Meraki Dashboards	87
Integrate the Meraki Dashboard	87
Update Meraki Dashboard Credentials	87
Manage Firepower Management Center	88
Integrate Firepower Management Center	88
Update Firepower Management Center Credentials	88
Filter Devices	89
Manage Devices in Inventory	90
Add a Device to a Site	90
Tag Devices	91
Tag Devices Using Rules	92
Edit Device Tags	92
Delete Tags	93
Configure a REP Ring for Devices	93
Create Port Groups	94
Assign Tags to Ports	95
Port Usage Information	95
Maintenance Mode for Devices	96
Schedule Maintenance for Devices	96
Manage Maintenance Schedule for Devices	97
Inventory Insights	97
Speed/Duplex Settings Mismatch	98

VLAN Mismatch	98
Manage System Beacon	99
Change the Device Role (Inventory)	99
Update a Device's Management IP Address	100
Update the Device Polling Interval	101
Resynchronize Device Information	102
Delete a Network Device	102
Launch Command Runner (Inventory)	103
Troubleshoot Device Reachability Issues Using Run Commands	103
Use a CSV File to Import and Export Device Configurations	104
Import Device Configurations from a CSV File	105
Export Device Data	105
Export Device Credentials	106
Configuration Drift of a Device	106
View Configuration Drift of a Device	107
Label Configuration Drift	108
Replace a Faulty Device	109
Replace a Faulty Access Point	111
Limitations of the RMA Workflow in Cisco DNA Center	112
Reboot Access Point	113

CHAPTER 6

Display Your Network Topology	115
About Topology	115
Display the Topology of Areas, Sites, Buildings, and Floors	116
Filter Devices on the Topology Map	116
Display Device Information	117
Display Link Information	118
Pin Devices to the Topology Map	119
Assign Devices to Sites	119
Save a Topology Map Layout	119
Open a Topology Map Layout	120
Share a Topology Map Layout	120
Export the Topology Layout	121

PART III**Design Your Network 123**

CHAPTER 7**Design the Network Hierarchy 125**

- Network Hierarchy Overview 125
- Design a New Network Hierarchy 126
- Use an Existing Cisco Network Hierarchy 126
 - Export Your Site Hierarchy from Cisco Prime Infrastructure 127
 - Export Your Map Archive from Cisco Prime Infrastructure 127
 - Import Your Site Hierarchy to Cisco DNA Center 128
 - Import Your Map Archive to Cisco DNA Center 129
- Use an Existing Ekahau Network Hierarchy 129
 - Export an Ekahau Project 129
 - Import an Ekahau Project to Cisco DNA Center 130
 - Import an Ekahau Site Survey to Cisco DNA Center 131
- Export Your Network Hierarchy from Cisco DNA Center 132
 - Export Your Site Hierarchy from Cisco DNA Center 133
 - Export Your Map Archive from Cisco DNA Center 133
- Search the Network Hierarchy 134
- Create a New Network Hierarchy 134
 - Create, Edit and Delete a Site 134
 - Add, Edit, and Delete a Building 135
 - Add, Edit, and Delete a Floor 136

CHAPTER 8**Work with Wireless 2D and 3D Floor Maps 139**

- Work with Floor Maps 139
- Add a Floor with a Map File 140
 - Floor Map Creation Methods 140
 - Guidelines for Image Files to Use in Maps 141
 - Add a Floor with a CAD Map File 141
 - Add a Floor with a Non-CAD Map File 142
- Work with 2D Maps 145
 - 2D Floor Map Devices and Overlay Objects 145
 - Work with APs on a Floor Map 146

Export Bulk APs from Cisco Prime Infrastructure and Import into Cisco DNA Center	146
Add APs to a Map	147
Add Planned APs to a Map	148
Assign Actual APs to Planned APs	149
Position an AP on a Map	150
Reposition an AP on a Map	151
Edit an AP	152
Edit Multiple APs	153
Remove APs from a Map	155
Work with Sensors on a Floor Map	155
Add Sensors to a Map	155
Position Sensors on a Map	156
Reposition a Sensor on a Map	156
Remove Sensors from a Map	157
Add, Edit, and Remove Coverage Areas	157
Add, Edit, Copy, and Remove Openings	158
Add, Edit, and Remove Location Regions	159
Add, Edit, and Remove an Inclusion Region	159
Add, Edit, and Remove an Exclusion Region	159
Add, Edit, and Remove Walls	160
Add, Copy, Edit, and Remove Shelving Units	161
Add, Edit, and Remove Markers	162
Add, Edit, and Remove GPS Markers	162
Add, Edit, and Remove Align Points	163
View a 2D Wireless Floor Map	163
2D Map Toolbar	165
2D Map View Options	167
2D Map Navigation Controls	169
AP Icon Legend	170
Filter Device Data on a Floor	171
Identify Wireless Interferers on the Floor Map	172
Work with 3D Maps	172
Configure Floor Map Elements and Overlays in 3D Maps	173
Clone an AP	173

View a 3D Wireless Map	174
3D Wireless Map Toolbar	175
3D Map View Options	176
3D Map Navigation Controls	179
Use First-Person and Third-Person Views for 3D Wireless Maps	183
Display Details About APs and Clients	185
Gain Insights from a 3D Wireless Map	186
Run the Wireless Coverage Optimizer	187
Create Simulations for 3D Wireless Maps	188

CHAPTER 9
Configure Network Settings 191

Network Settings Overview	191
Add Cisco ISE or Other AAA Servers	192
Configure Global Network Servers	193
Global Device Credentials Overview	194
Configure Global CLI Credentials	194
Configure Global SNMPv2c Credentials	195
Configure Global SNMPv3 Credentials	195
Configure Global HTTPS Credentials	197
Guidelines for Editing Global Device Credentials	199
Edit Global Device Credentials	199
Associate Device Credentials to Sites	200
Manage Device Credentials	200
Configure IP Address Pools	202
Import IP Address Pools from an IP Address Manager	202
Import IP Address Pools from a CSV File	203
Reserve an IP Address Pool	203
Edit IP Address Pools	204
Delete IP Address Pools	204
Clone an IP Address Pool	205
Release IP Address Pools	205
View IP Address Pools	205
Configure Service Provider Profiles	207
Configure Global Wireless Settings	207

Create SSIDs for an Enterprise Wireless Network	207
Preshared Key Override	213
Create Pre-Auth Access Control Lists	213
Configure AAA Server for an Enterprise Wireless Network	215
Create SSIDs for a Guest Wireless Network	216
Configure AAA Server for a Guest Wireless Network	223
Create SSID Scheduler	225
Create a Wireless Interface	225
Design and Provision Interface/VLAN Groups to Nonfabric Deployments	226
Create a Wireless Radio Frequency Profile	227
Edit or Delete a Basic Radio Frequency Profile	235
Prerequisites for Configuring AI Radio Frequency Profiles	236
Create an AI Radio Frequency Profile	237
Edit an AI Radio Frequency Profile	244
Delete an AI Radio Frequency Profile	245
Configure an AI Radio Frequency Profile	245
Assign a Location to an Existing AI RF Profile	247
Unassign a Location from an Existing AI RF Profile	248
Upgrade a Basic Radio Frequency Profile to an AI Radio Frequency Profile	249
Create an AP Authorization List	250
Edit or Delete an AP Authorization List	251
Create an Anchor Group	252
Edit or Delete an Anchor Group	253
AP Profiles	253
Create an AP Profile for Cisco IOS XE Devices	254
Create an AP Profile for Cisco AireOS Devices	260
Edit or Delete an AP Profile	262
Create an AP Power Profile	262
Edit or Delete an AP Power Profile	263
Provision a Cisco Sensor SSID for Nonfabric Deployment	263
Manage Backhaul Settings	265
About Cisco Connected Mobile Experiences Integration	266
Create Cisco CMX Settings	266
About Cisco Spaces Integration	268

Assign Cisco Spaces to Sites	269
Monitor Sites Using Cisco Spaces	269
Configure a FlexConnect VLAN	270
About Wireless Mesh Networks	271
Configure a Certificate Revocation Check	273

CHAPTER 10
Configure Network Profiles 275

Network Profiles Overview	275
Create Network Profiles for Assurance	275
Create Network Profiles for Firewall	277
Create Network Profiles for Routing	278
Create Network Profiles for Switching	280
Create Network Profile for Cisco DNA Traffic Telemetry Appliance	281
Create Network Profiles for Wireless	281
Add SSIDs to a Network Profile	282
Add AP Zones to a Network Profile	283
Add Model Configurations to a Network Profile	284
Add Templates to a Network Profile	285
Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile	285

PART IV
Configure and Maintain Network Devices 289

CHAPTER 11
Create Templates to Automate Device Configuration Changes 291

About Template Hub	291
Create Projects	293
Create Templates	293
Create a Regular Template	293
Blocked List Commands	295
Sample Templates	295
Create a Composite Template	295
Edit Templates	297
Template Simulation	297
Export Template(s)	298
Import Template(s)	299

Clone a Template	299
Attach a CLI Template to the Network Profiles	300
Provision CLI Templates	301
Export Project(s)	301
Import Project(s)	301
Template Variables	302
Variable Binding	303
Special Keywords	306
Associate Templates to Network Profiles	309
Detect Conflicts in a CLI Template	310
Potential Design Conflicts Detection Between CLI Template and Service Provisioning Intent	311
Detect CLI Template Run-Time Conflict	311

CHAPTER 12**Design Model Configuration 313**

Introduction to Model Config Editor	313
Supported Model Config Design Types	314
Discover and Create Designs from a Legacy Device	314
Create a Model Config Design for AAA RADIUS Attributes	314
Create a Model Config Design for Advanced SSID	315
Create a Design for Cisco CleanAir	319
Create a Model Config Design for Dot11ax Configuration	321
Create a Model Config Design for Event-Driven RRM	322
Create a Design for Flex Configuration	324
Create a Design for Global IPv6	326
Create a Model Config Design for Multicast	326
Create a Model Config Design for RRM FRA Parameters	328
Create a Model Config Design for RRM General Parameters	329

CHAPTER 13**Manage Software Images 331**

About Image Repository	331
Integrity Verification of Software Images	332
View Software Images	332
Use a Recommended Software Image	335
Import a Software Image	335

Assign a Software Image to a Device Family	336
Upload Software Images for Devices in Install Mode	337
About Golden Software Images	337
Specify a Golden Software Image	338
Configure an Image Distribution Server	339
Change the Protocol Order of an Image Distribution Server	340
Add Image Distribution Servers to Sites	340
Provision a Software Image	341
Import the ISSU Compatibility Matrix	343
Upgrade a Software Image with ISSU	343
List of Device Upgrade Readiness Prechecks	345
View Image Update Status	346
View Image Update Workflow	346
Auto Flash Cleanup	348

CHAPTER 14	Compliance Audit for Network Devices	349
	Compliance Overview	349
	Types of Compliance	350
	View Compliance Summary	353
	Manual Compliance Run	354
	Generate a Compliance Audit Report for Network Devices	354
	Acknowledge Compliance Violations	355
	Synchronize Startup and Running Configurations of a Device	356
	Fix Compliance Violations	356
	Compliance Behavior After Device Upgrade	357
	Limitations in CLI Template Compliance	358

CHAPTER 15	Run Diagnostic Commands on Devices	361
	Command Runner Overview	361
	Run Diagnostic Commands on Devices	361

PART V	Provision Your Network	363
---------------	-------------------------------	------------

CHAPTER 16	Onboard and Provision Devices with Plug and Play	365
-------------------	---	------------

Plug and Play Provisioning Overview	365
Plug and Play Provisioning Prerequisites	367
DHCP Controller Discovery	369
DNS Controller Discovery	370
Plug and Play Connect Controller Discovery	371
Plug and Play Deployment Guidelines	372
View Devices	372
Add or Edit a Device	374
Add Devices in Bulk	375
Register or Edit a Virtual Account Profile	376
Add Devices from a Smart Account	377
Provision a Device with Plug and Play	378
Provision a Switch or Router Device	379
Provision a Wireless or Sensor Device	383
Provision a Cisco DNA Traffic Telemetry Appliance	385
Complete the Provisioning Process	386
Delete a Device	387
Reset a Device	387

CHAPTER 17
Provision Wireless Devices 389

Wireless Device Provisioning Overview	389
About Wireless Devices and Country Codes	389
Prerequisites for Provisioning a Cisco AireOS Controller	390
Provision a Cisco AireOS Controller	391
Configure Cisco Wireless Controller High Availability	394
Prerequisites for Configuring Cisco Wireless Controller High Availability	394
Configure Cisco Wireless Controller HA	395
What Happens During or After the High Availability Process is Complete	396
Commands to Configure and Verify High Availability	396
Disable High Availability Configured Device in the Existing Deployment	396
Provision a Cisco AP—Day 1 AP Provisioning	397
Enable ICMP Ping on APs in FlexConnect Mode	399
Day 0 Workflow for Cisco AireOS Mobility Express APs	399
Provision Cisco AireOS Controllers in the Existing Deployment	401

Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller	403
Cisco Catalyst 9800 Series Wireless Controller Overview	403
Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center	406
Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller	409
Configure High Availability for the Cisco Catalyst 9800 Series Wireless Controller	410
Information About High Availability	412
Commands to Configure High Availability on Cisco Catalyst 9800 Series Wireless Controllers	412
Commands to Verify Cisco Catalyst 9800 Series Wireless Controllers High Availability	413
N+1 High Availability	413
Overview of N+1 High Availability	413
Prerequisites for Configuring N+1 High Availability from Cisco DNA Center	414
Configure N+1 High Availability from Cisco DNA Center	415
Mobility Configuration Overview	416
Mobility Configuration Workflow	417
Mobility Configuration Use Cases	417
Configure Mobility Group	418
About DTLS Ciphersuites	419
Configure Multiple DTLS Ciphersuites	420
About N+1 Rolling AP Upgrade	421
Workflow to Configure a Rolling AP Upgrade	421
Provision a Cisco Catalyst 9800 Series Wireless Controller	423
Configure Cisco Wireless Controllers on the Existing Infrastructure	425
Day 0 Workflow for Cisco Embedded Wireless Controller on Catalyst Access Points	427
Migrate Cisco AireOS Controller to Cisco Catalyst 9800 Series Wireless Controller Using Cisco DNA Center	429
Configure and Provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches	431
Supported Hardware Platforms	431
Preconfiguration	433
Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches	433
Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches	435
Inter-Release Controller Mobility Introduction	437
Guest Anchor Configuration and Provisioning Process	438
Prerequisite for Configuring IRCM on Cisco Controller Device	439

- IRCM: Cisco AireOS Controller and Cisco Catalyst 9800 Series Wireless Controller 439
- Prerequisites for Provisioning a Meraki Device 440
- Provision a Meraki Device 441
- Provision Remote Teleworker Devices 443
 - Remote Teleworker Deployment Overview 443
 - Create a Remote Teleworker Site 444

CHAPTER 18 **Provision a Routing Profile 447**

- Provision a Router 447
- VPC Inventory Collection 449

CHAPTER 19 **Provision Firewall Profiles 451**

- Provision a Firewall Threat Defense Device 451

CHAPTER 20 **Provision a LAN Underlay 453**

- LAN Automation 453
- Prerequisites for Provisioning a Network Through LAN Automation 454
- Provision a Network Through LAN Automation 455
- Peer Device in LAN Automation Use Case 458
- Check the LAN Automation Status 460
- Create a Link Between Interfaces 460
- Delete a Link Between Interfaces 461

CHAPTER 21 **Provision Fabric Networks 463**

- Cisco SD-Access Zero-Trust Security Solution 463
 - Zero-Trust Overview Dashboard 464
 - Day 0 View of Zero-Trust Overview Dashboard 464
 - Get Started with SD-Access Zero-Trust Workplace Journey 466
 - Day n View of Zero-Trust Overview Dashboard 467
 - Modify SD-Access Zero-Trust Workplace Journey 469
- About Fabric Networks 470
 - Fabric Sites 471
 - Transits 471
 - Fabric Readiness and Compliance Checks 471

New Automation for SD-Access	472
Add a Fabric Site	473
Configure Devices for a Fabric Site	474
Add a Device to a Fabric	475
Add a Device as a Border Node	476
Configure LISP Pub/Sub	479
Create an IP Transit	480
Create an SD-Access Transit	480
Select an Authentication Template	481
Configure Ports Within the Fabric Site	482
Configure Wireless SSIDs for Fabric Networks	483
Virtual Networks	484
Create a Layer 3 Virtual Network	484
Create a Layer 2 Virtual Network	485
Associate Layer 3 Virtual Networks to Fabric Sites	486
Create Anycast Gateways	487
Virtual Network Policy	489
Guidelines to Configure a Virtual Network Policy	489
Create a Virtual Network Policy	489
Edit a Virtual Network Policy	490
Delete a Virtual Network Policy	490
Configure a Fabric Zone	490
Create a Fabric Site and Its Fabric Zones	491
Create a Fabric Zone Within a Fabric Site	492
Associate Layer 3 Virtual Networks to Fabric Zones	493
Associate Layer 2 Virtual Networks to Fabric Zones	494
Associate Anycast Gateways to Fabric Zones	495
Configure an Extended Node Device	496
Steps to Configure an Extended Node	496
Upgrade an Extended Node to a Policy Extended Node	498
Delete an Extended Node	499
Configure a REP Ring Topology for Extended Nodes and Policy Extended Nodes	500
View REP Ring Status	501
Delete a REP Ring	502

Delete a Node from a REP Ring	502
Configure Supplicant-Based Extended Nodes	502
Steps to Configure a Supplicant-Based Extended Node	503
Replace a Faulty Port	504
Configure Cisco Identity Services Engine to Onboard Supplicant-Based Extended Node	505
Configure a Port Channel	509
Create a Port Channel	509
Update a Port Channel	510
Delete a Port Channel	510
Multicast	510
Configure Multicast	511

CHAPTER 22
Provision Services 513

Applications	513
About Application Visibility	513
Day 0 Setup Wizard to Enable the Application Visibility Service	514
Day-N Application Visibility View	515
Reconfigure CBAR	518
Applications and Application Sets	518
Unidirectional and Bidirectional Application Traffic	518
Custom Applications	519
Discovered Applications	519
Favorite Applications	519
Configure Applications and Application Sets	520
Change an Application's Settings	520
Create a Server Name-Based Custom Application	521
Create an IP Address and Port-Based Custom Application	521
Create a URL-Based Custom Application	522
Edit or Delete a Custom Application	523
Mark an Application as Favorite	523
Create a Custom Application Set	524
Edit or Delete a Custom Application Set	524
Update the Protocol Pack on a CBAR-Enabled Device	525
Discover Unclassified Applications	525

Configure the NBAR Cloud Connector	526
Application Visibility Service Support for the Cisco DNA Traffic Telemetry Appliance	527
Discover Infoblox Applications	527
Resolve Unclassified Traffic Using Microsoft Office 365 Cloud Connector	528
Edit or Delete a Discovered Application	529
Application Hosting	529
About Application Hosting	529
Install or Update the Application Hosting Service Package	530
Prerequisites for Application Hosting	530
View Device Readiness to Host an Application	531
Add an Application	531
Automatic Download of ThousandEyes Enterprise Agent Application	532
Update an Application	532
Start an Application	533
Stop an Application	533
View Applications Hosted on Device	533
Install an Application on a Cisco Catalyst 9300 Device	534
Uninstall an Application from a Cisco Catalyst 9300 Device	535
Edit an Application Configuration in a Cisco Catalyst 9300 Device	535
Delete an Application	536
Download App Logs	536
Download Device Tech Support Logs	536
Application Hosting on Cisco Catalyst 9100 Series Access Points	537
About Application Hosting on Cisco Catalyst Access Points	537
Application Hosting Workflow to Install and Manage USB on Cisco Catalyst 9100 Series Access Points	537
View Installed Hosting Applications on Cisco Catalyst 9100 Series Access Points	538
Uninstall an Application from a Cisco Catalyst 9100 Device	539
Delete an Application from a Cisco Catalyst 9100 Device	539
Configure a Site-to-Site VPN	539
Create a Site-to-Site VPN	540
Edit a Site-to-Site VPN	540
Delete a Site-to-Site VPN	541
Create a User-Defined Network Service	541

- View the User-Defined Network Service Provisioning Status 541
- Enable Telemetry on Switches 542
- Configure Cisco Umbrella 543
 - About Cisco Umbrella 543
 - Role-Based Access Control Settings for Cisco Umbrella 543
 - Configure Cisco Umbrella with Cisco DNA Center 544
 - Add the Umbrella Dashlet 544
 - View the Umbrella Service Statistics Dashboard 545
 - Prerequisites for Provisioning Cisco Umbrella on Network Devices 545
 - Provision Cisco Umbrella on Network Devices 546
 - Disable Cisco Umbrella on Network Devices 547
 - Update the Cisco Umbrella Configuration on Network Devices 548
- Create Secure Tunnel 550
 - Configure Secure Tunnel 550

PART VI

Configure Policies 553

CHAPTER 23

Configure Group-Based Access Control Policies and Analytics 555

- Group-Based Access Control 555
 - Group-Based Access Control Policy Dashboard 556
 - Group-Based Access Control Policies 557
 - Policy Creation Overview 560
 - Create a Security Group 560
 - Edit a Security Group 561
 - Delete a Security Group 562
 - Synchronization of Security Groups Between Cisco DNA Center and Cisco ISE 562
 - Create an Access Contract 563
 - Edit an Access Contract 564
 - Delete an Access Contract 564
 - Synchronization of Access Contracts Between Cisco DNA Center and Cisco ISE 565
 - Create Group-Based Access Control Policy 565
 - Update a Group-Based Access Control Policy Based on Traffic Flows 567
 - Synchronization of Policies Between Cisco DNA Center and Cisco ISE 568
- Cisco Group-Based Policy Analytics 568

About Cisco Group-Based Policy Analytics	568
Install Group-Based Policy Analytics	569
Hardware and Software Compatibility	569
Understand Connectors	571
Initial Configuration of Cisco Group-Based Policy Analytics	572
Explore Groups and Endpoints	573
Multiple Groups to Multiple Groups	573
Single Group to Multiple Groups	574
Single Group to Single Group	575
Access Contracts	577
Date and Time Selector	579
Use Search	579
Role-Based Access Control	581

CHAPTER 24
Configure IP-Based Access Control Policies 583

IP-Based Access Control Policies	583
Workflow to Configure an IP-Based Access Control Policy	584
Configure Global Network Servers	584
Create an IP Network Group	585
Edit or Delete an IP Network Group	585
Create an IP-Based Access Control Contract	585
Edit or Delete an IP-Based Access Control Contract	586
Create an IP-Based Access Control Policy	586
Edit or Delete an IP-Based Access Control Policy	588
Deploy an IP-Based Access Control Policy	588

CHAPTER 25
Configure Application Policies 589

Application Policies Overview	589
CVD-Based Settings in Application Policies	590
Site Scope	590
Business-Relevance Groups	590
Consumers and Producers	591
Marking, Queuing, and Dropping Treatments	591
Service Provider Profiles	593

Queuing Profiles	595
Processing Order for Devices with Limited Resources	596
Policy Drafts	598
Policy Preview	599
Policy Precheck	599
Policy Scheduling	599
Policy Versioning	599
Original Policy Restore	600
Stale Application Policies	600
Application Policy Guidelines and Limitations	601
Manage Application Policies	602
Prerequisites	602
Create an Application Policy	602
View Application Policy Information	605
Edit an Application Policy	606
Save a Draft of an Application Policy	607
Deploy an Application Policy	607
Cancel a Policy Deployment	608
Delete an Application Policy	608
Clone an Application Policy	609
Restore an Application Policy	609
Reset the Default CVD Application Policy	610
Preview an Application Policy	610
Precheck an Application Policy	611
Display Application Policy History	611
Roll Back to a Previous Policy Version	611
Manage Queuing Profiles	612
Create a Queuing Profile	612
Edit or Delete a Queuing Profile	613
Manage Application Policies for WAN Interfaces	613
Customize Service Provider Profile SLA Attributes	613
Assign a Service Provider Profile to a WAN Interface	614

Traffic Copy Policies	617
Sources, Destinations, and Traffic Copy Destinations	617
Guidelines and Limitations of Traffic Copy Policy	618
Workflow to Configure a Traffic Copy Policy	618
Create a Traffic Copy Destination	619
Edit or Delete a Traffic Copy Destination	619
Create a Traffic Copy Contract	619
Edit or Delete a Traffic Copy Contract	620
Create a Traffic Copy Policy	620
Edit or Delete a Traffic Copy Policy	620

PART VII
Monitor and Troubleshoot Your Network 623

CHAPTER 27
Cisco AI Endpoint Analytics 625

Cisco AI Endpoint Analytics Overview	625
Key Features of Cisco AI Endpoint Analytics	626
FIPS Compliance	627
Set Up Cisco AI Endpoint Analytics in Cisco DNA Center	628
Install Software Updates	628
Connect and Enable Data Sources	629
Endpoint Telemetry Sources	631
Cisco AI Endpoint Analytics Overview Window	632
Integrate Cisco AI Endpoint Analytics with Talos Intelligence	633
Publish Authorization Attributes to Cisco ISE	636
Trust Analytics	637
Customize Impact Level	637
Configure Reset Alert	638
Endpoint Purge Policies	639
Create a Purge Policy	640
Configure Endpoint Subnet Inspection	640
Endpoint Inventory	641
Export Cisco AI Endpoint Analytics Data	642
Filter Endpoints	643
Attribute Glossary	644

Register Endpoints	644
Edit Registered Endpoints	645
Delete Registered Endpoints	645
Trust Score	645
Trust Scores for Endpoints	646
Endpoint Attribute Conflict	650
NAT Mode Detection	650
Endpoints with Concurrent MAC Addresses Connected to Cisco Catalyst 9000 Series Devices	651
Initial Trust Score Assessment Using Posture and Authentication Values from Cisco ISE	652
Trust Scores for Endpoints with Random and Changing MAC Addresses	652
Sensor Scans to Check for Open Ports and Credential Vulnerabilities	653
View and Manage Trust Scores for Endpoints	655
Control Endpoint Spoofing	660
Profiling Rules	661
Rule Prioritization	662
Filter Profiling Rules	662
View Updated Profiling Rules	662
System Rules	663
Automatic System Rule Updates for Endpoint Profiling	663
Custom Rules	664
Logic and Conditions for Profiling Rules	664
Create a Custom Rule	665
Edit a Custom Rule	665
Delete a Custom Rule	666
Export and Import Custom Profiling Rules Across Deployments Using APIs	666
Cisco AI Rules for Smart Grouping	667
New Profiling Suggestions for Similar Endpoints in Your Network	667
Smart Modification Suggestions for Your Endpoint Profiling Rules	669
Smart Suggestions to Delete Profiling Rules	671
Import Profiling Rules	673
Export Profiling Rules	673
Hierarchy	673
Create Category and Subcategory	673
Edit a Category or Subcategory	674

Delete Endpoint Types from Category	674
Reassign Endpoint Types from Category	674
Delete a Category	675

CHAPTER 28**Troubleshoot Network Devices Using Network Reasoner 677**

Network Reasoner Overview	677
Validate Cisco SD-Access Migration Using the MRE Workflow	677
Troubleshoot High CPU Utilization	679
Troubleshoot a Power Supply Failure	680
Troubleshoot a Downed Interface	681
Troubleshoot Network Connectivity	682
Troubleshoot IP Connectivity of a Device	683
Troubleshoot Wireless Clients Using the MRE Workflow	683
Troubleshoot Wireless APs Using the MRE Workflow	684
Troubleshoot Unmonitored Devices Using the MRE Workflow	685
Scan the Network for Bugs	686
Scan Cisco DNA Center for Bugs	689

CHAPTER 29**Identify Network Security Advisories 691**

Security Advisories Overview	691
Prerequisites	691
View Security Advisories	692
Schedule a Security Advisories Scan	693
Enable the Try Cisco CX Cloud Success Track to Identify Security Advisories	694
CLI Commands Invoked for Security Advisories	695
Rescan the Network to Identify Security Advisories	695
Hide and Unhide Devices from an Advisory	696
Hide and Unhide Advisories from a Device	696
Add Notification for a New Security Advisory KB	697
View Security Advisories in the Inventory	698
Add a Match Pattern	698
Define AND/OR for the Match Pattern	699
Edit the Match Pattern	699
Delete the Match Pattern	700

PART VIII	Assure Your Network	701
------------------	----------------------------	------------

CHAPTER 30	Cisco DNA Assurance	703
	Overview of Cisco DNA Assurance	703

PART IX	Manage Cisco DNA Center	705
----------------	--------------------------------	------------

CHAPTER 31	Build and Deploy Workflows	707
	Cisco DNA Center Workflow Navigation	707
	Discover Devices	707
	AP Refresh Workflow	709
	Configure User-Defined Network Workflow	711
	Overview of User-Defined Network Service	711
	Prerequisites for Configuring the User-Defined Network Service	711
	Configure Cisco User-Defined Network	712
	Enable Application Hosting on Switches	714
	Enable IoT Services Workflow	715
	Enable IoT Services on Cisco Catalyst 9100 Series Access Points	715
	Manage IoT Applications	716
	AP Configuration in Cisco DNA Center	716
	Configure AP Workflow	716
	Schedule Recurring Events for AP Workflow	723
	Learn Device Configurations from Devices with Pre-Existing Infrastructure	724
	Replace Device Workflow	729
	Create a Remote Support Authorization	731
	Create an Event Notification	732
	Configure Remote LAN	735
	Workflow to Create an IP- and URL-Based Access Control Policy	737

CHAPTER 32	Troubleshoot Cisco DNA Center Using Data Platform	739
	About Data Platform	739
	Troubleshoot Using the Analytics Ops Center	740
	View or Update Collector Configuration Information	741

[View Data Retention Settings](#) 742

[View Pipeline Status](#) 743



CHAPTER 1

New and Changed Information

- [New and Changed Information](#) , on page 1

New and Changed Information

The following tables summarize the new and changed features in Cisco DNA Center and tell you where they are documented.

Table 1: New and Changed Features for Cisco DNA Center, Release 2.3.5.5

Feature	Description
Recommended Release	Cisco DNA Center 2.3.5.5 contains fixes for critical issues. We recommend that customers on all earlier Cisco DNA Center releases, including the 2.3.5.x releases, upgrade to Cisco DNA Center 2.3.5.5.
Enhancements to Default AP Profiles During Upgrade	In earlier releases, the default AP profile was pushed to the wireless controller during upgrade. When you upgrade to this release from an earlier version, by default, Cisco DNA Center doesn't push the default AP profile to the wireless controller. To update the default AP profile on the wireless controller, you must explicitly save it on the Design > Network Settings > Wireless > AP Profiles window. After you save the default AP profile, if there is a difference between the current wireless controller configuration and the AP profile configuration saved on Cisco DNA Center, the default AP profile is pushed to the wireless controller during subsequent reprovisioning. See AP Profiles , on page 253.

Table 2: New and Changed Features for Cisco DNA Center, Release 2.3.5.4

Feature	Description
Ability to Assign Ports for Uplink Ports	Effective with this release, you can assign ports for the uplink ports. Choose Provision > Fabric Sites and click the fabric site. Under Host Onboarding > Port Assignment , assign ports for the uplink ports. In earlier releases, you could assign ports for the uplink ports only for extended node devices.

Feature	Description
AP Location Configuration for PnP Onboarding	<p>Effective with this release, you can configure the site assigned during the PnP claim as the AP location for PnP onboarding.</p> <p>See Plug and Play Provisioning Prerequisites, on page 367 and Provision a Wireless or Sensor Device, on page 383.</p>
Enhancements to Access Control Lists for Central Web Authentication SSIDs of Guest Wireless Network	<p>Effective with this release, Cisco DNA Center-generated preauthentication Access Control Lists (ACL) are created only for the configured AAA or PSN servers for Central Web Authentication (CWA) SSIDs of guest wireless networks.</p> <p>See Configure AAA Server for a Guest Wireless Network, on page 223.</p>
Enhancements to Admin Status of Radio Bands in RF Profiles for Cisco AireOS Wireless Controllers	<p>Effective with this release, for Cisco AireOS Wireless Controllers, if you disable the Admin status of a band in the RF profile and reprovision the wireless controller or AP, Cisco DNA Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as None) and disables the Admin status of all radios of the corresponding band on the APs.</p> <p>See Create a Wireless Radio Frequency Profile, on page 227.</p>
Enhancements to RF Profile Updates for Cisco AireOS Wireless Controllers	<p>In earlier releases, for Cisco AireOS Wireless Controllers, if you modify any configuration in an RF profile that is already provisioned on a wireless controller, Cisco DNA Center resets the corresponding radio.</p> <p>Effective with this release, for Cisco AireOS Wireless Controllers, if you modify the DCA channels or data rates for an RF profile that is already provisioned on a wireless controller, Cisco DNA Center resets the corresponding radio.</p> <p>See Edit or Delete a Basic Radio Frequency Profile, on page 235.</p>
Support for Manual Data Refresh to Track the Replacement Status in the AP Refresh Workflow	<p>In the Access Point Refresh workflow, to view the latest AP replacement status, you can use the Refresh Data option.</p> <p>Note Effective with this release, Cisco DNA Center doesn't refresh the data automatically.</p> <p>See AP Refresh Workflow, on page 709.</p>
Support for Static IP Address for Wireless Management Interface During Provisioning of Cisco Catalyst 9800 Series Wireless Controller	<p>Effective with this release, you must configure a static IP address for the wireless management interface on the Cisco Catalyst 9800 Series Wireless Controller to prevent provisioning failure.</p> <p>See Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center, on page 406.</p>

Table 3: New and Changed Features for Cisco DNA Center, Release 2.3.5.3

Feature	Description
Dynamic Channel Assignment (DCA) Validation	<p>DCA channel support is based on the regulatory domain of the device. During AP provisioning with an RF profile selected, out of all the DCA channels configured on the RF profile only the supported channels as per the country code are considered and the unsupported channels are ignored. You can view the list of unsupported channels in the AP preprovision summary window.</p> <p>See Create a Wireless Radio Frequency Profile, on page 227, Create an AI Radio Frequency Profile, on page 237, and About Wireless Devices and Country Codes, on page 389.</p>
Enhancements to Accounting Server Configuration	<p>Effective with this release, you must configure an accounting server for an SSID to push the accounting configuration for the SSID.</p> <p>See Configure AAA Server for an Enterprise Wireless Network, on page 215 and Configure AAA Server for a Guest Wireless Network, on page 223.</p>
Enhancements to AP Configuration Workflow	<p>The Configure Access Points workflow has the following enhancements:</p> <ul style="list-style-type: none"> • The Antenna Name parameter has been replaced with the Antenna Gain parameter. The antenna name selected in this workflow isn't reflected in wireless maps. • The AP Height, Azimuth, and Elevation parameters have been removed. You can configure these parameters in the Design > Network Hierarchy window. • You can select a maximum of 2000 sites in the Select Access Points window. <p>See Configure AP Workflow, on page 716.</p>
Enhancements to AP Location Configuration	<p>During AP provisioning and AP Plug and Play (PnP) onboarding, Cisco DNA Center doesn't configure the assigned site as the AP location. You can configure the AP location using the Configure Access Points workflow.</p> <p>See Provision a Cisco AP—Day 1 AP Provisioning, on page 397, Provision a Wireless or Sensor Device, on page 383, and Configure AP Workflow, on page 716.</p>
Enhancements to Application Hosting on APs	<p>When the App Hosting Status of an AP is Ready, to configure the updates on the AP, you can use the Resync option.</p> <p>See View Installed Hosting Applications on Cisco Catalyst 9100 Series Access Points, on page 538.</p>
Enhancements to Authentication using AAA Server for Wireless Networks	<p>Effective with this release, you must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Cisco DNA Center pushes the aaa authentication dot1x default local command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.</p> <p>See Configure AAA Server for an Enterprise Wireless Network, on page 215 and Configure AAA Server for a Guest Wireless Network, on page 223.</p>

Feature	Description
Enhancements to Editing RF Profiles	<p>Effective with this release, when you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovisioning also pushes the RF profiles updates to the devices and AP reprovisioning is not necessary.</p> <p>If you don't need the RF profile updates during the wireless controller reprovisioning, you can check the Skip AP Provision check box.</p> <p>See Edit or Delete a Basic Radio Frequency Profile, on page 235 and Edit an AI Radio Frequency Profile, on page 244.</p>
Enhancements to RF Profiles	<p>Effective with this release, for Cisco Catalyst 9800 Series Wireless Controllers, disabling a radio band on the RF profile doesn't disable the Admin status of the respective radios on all APs that use the RF profile. Instead, Cisco DNA Center disables the Admin status of the corresponding RF profile.</p> <p>Note When the Admin status of a radio band on the RF profile is in disabled state and you upgrade to Release 2.3.5.3 from Release 2.3.3.6 or earlier, if you reprovision the wireless controller or AP:</p> <ul style="list-style-type: none"> • Cisco DNA Center creates the RF profile for the corresponding radio band with Admin status as disabled. • Cisco DNA Center updates the RF profile mapping in the RF tag on the device from Global Config to the newly created RF profile. <p>See Create a Wireless Radio Frequency Profile, on page 227 and Create an AI Radio Frequency Profile, on page 237.</p>
Enhancements to Site Tags, Policy Tags, and AP Zone Provisioning	<p>Site tags, policy tags, and AP zone provisioning have the following enhancements:</p> <ul style="list-style-type: none"> • If an AP zone is already provisioned on an AP and you update the AP zone configuration, you must reprovision the wireless controller. Reprovisioning the AP is not necessary. • Newly added custom site tag and policy tag configurations are applied only when you provision the APs. Provisioning the wireless controller alone doesn't configure the new custom tags on the APs. If there are any updates to the tags after the first provisioning, you must reprovision the wireless controller or APs. <p>See Add AP Zones to a Network Profile, on page 283 and Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 285.</p>

Table 4: New and Changed Features for Cisco DNA Center, Release 2.3.5.0

Feature	Description
Advanced WLAN Parameters Configuration Support for Enterprise and Guest Wireless Networks	<p>You can configure the following advanced WLAN parameters while creating SSIDs for enterprise and guest wireless networks:</p> <ul style="list-style-type: none"> • AAA Override • Configure MPSK • Protected Management Frame (802.11w) • Coverage Hole Detection <p>See Create SSIDs for an Enterprise Wireless Network, on page 207 and Create SSIDs for a Guest Wireless Network, on page 216.</p>
Basic RF Profile and AI RF Profile Enhancements	<p>You can configure the following settings for basic radio frequency (RF) profiles:</p> <ul style="list-style-type: none"> • Coverage hole detection • Flexible Radio Assignment (FRA) • 802.11ax <p>You can configure the following settings for AI RF profiles:</p> <ul style="list-style-type: none"> • Coverage hole detection • 802.11ax <p>See Create a Wireless Radio Frequency Profile, on page 227, Create an AI Radio Frequency Profile, on page 237, Create a Model Config Design for Dot11ax Configuration, on page 321, Create a Model Config Design for Advanced SSID, on page 315, and Create a Model Config Design for RRM FRA Parameters, on page 328.</p>
Cisco DNA Center Journey Map	<p>The Cisco DNA Center journey map shows various capabilities provided by Cisco DNA Center and its usage.</p> <p>See Cisco DNA Center Journey Map, on page 21.</p>
Client Rate Limit Configuration Support for Enterprise and Guest Wireless Networks	<p>You can configure the client rate limit on Cisco IOS XE devices while creating SSIDs for enterprise and guest wireless networks.</p> <p>See Create SSIDs for an Enterprise Wireless Network, on page 207 and Create SSIDs for a Guest Wireless Network, on page 216.</p>
Compliance Support Extended for Cisco Umbrella	<p>You can check compliance for switches or Cisco Embedded Wireless Controllers configured with Cisco Umbrella.</p> <p>You can view any violations under Workflow in the Compliance Summary window.</p> <p>See Types of Compliance, on page 350.</p>
Compliance Support Extended for Network Settings	<p>You can check compliance for device network settings.</p> <p>You can view any violations under Network settings in the Compliance Summary window.</p> <p>See Types of Compliance, on page 350.</p>

Feature	Description
Detect Conflicts in a CLI Template	<p>You can detect potential design conflicts and run-time conflicts in the CLI templates for switching, SD-Access, and fabric.</p> <p>See Detect Conflicts in a CLI Template, on page 310, Potential Design Conflicts Detection Between CLI Template and Service Provisioning Intent, on page 311, and Detect CLI Template Run-Time Conflict, on page 311.</p>
Enhanced Multicast Capabilities in Cisco SD-Access fabric	<p>Cisco SD-Access multicast capabilities are enhanced to accommodate multiple external RP configuration, ASM group-to-RP mapping, and concurrent ASM, SSM configuration per Layer 3 virtual network.</p> <p>See Configure Multicast, on page 511.</p>
Enhancements to Default Configuration of Fast Transition Over Distributed Systems for SSIDs	<p>Effective with this release, fast transition over a distributed system (Over the DS check box) is disabled by default for SSIDs for guest and enterprise wireless networks.</p> <p>See Create SSIDs for an Enterprise Wireless Network, on page 207 and Create SSIDs for a Guest Wireless Network, on page 216.</p>
Exclude Interfaces in Application Visibility Service Enablement	<p>You can exclude or include interfaces in the Application Visibility service enablement.</p> <p>See Day 0 Setup Wizard to Enable the Application Visibility Service, on page 514.</p>
Fix Compliance Violations	<p>Cisco DNA Center provides you with an automated fix for device compliance violations that are identified during a compliance run.</p> <p>See Fix Compliance Violations, on page 356.</p>
HTTPS Protocol Support for Software Image Management	<p>HTTPS protocol support is extended for software image management on Cisco Embedded Wireless Controllers.</p> <p>See Change the Protocol Order of an Image Distribution Server, on page 340.</p>
<p>LAN Automation Enhancements:</p> <ul style="list-style-type: none"> • New GUI • Support for Multiple LAN Automation Sessions 	<p>A new user interface window for LAN Automation supports both Day 0 and Day N operations, such as:</p> <ul style="list-style-type: none"> • Start and stop LAN Automation session • Add and delete a Layer 3 interface link • View the newly discovered devices • View the provisioned devices • Check the history of LAN Automation sessions • View the session logs, logs for newly discovered devices, and so on <p>You can run multiple (a maximum of five) LAN Automation sessions simultaneously, across sites. However, you can enable only one LAN Automation session per site.</p> <p>See LAN Automation, on page 453, Provision a Network Through LAN Automation, on page 455, Create a Link Between Interfaces, on page 460, and Delete a Link Between Interfaces, on page 461.</p>

Feature	Description
PSC Enforcement Support for RF Profiles	<p>You can enable Preferred Scanning Channel (PSC) enforcement for the 6-GHz radio type for basic RF profiles and AI RF profiles.</p> <p>See Create a Wireless Radio Frequency Profile, on page 227 and Create an AI Radio Frequency Profile, on page 237.</p>
Resilient Ethernet Protocol (REP) Ring Device Support (Nonfabric)	<p>REP Ring support for nonfabric devices is extended for S5800.</p> <p>See Configure a REP Ring for Devices, on page 93.</p>
Support for AP Authorization Configuration	<p>You can configure a list of authorized APs. You can configure local and AAA authorization for APs using their MAC address, serial number, or both.</p> <p>See Create an AP Authorization List, on page 250, Provision a Cisco AireOS Controller, on page 391, and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423.</p>
Support for AP Power Profiles	<p>You can create AP power profiles for Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later. You can assign the AP power profile to APs by associating it with an AP profile. You can define multiple rules for the AP power profile and specify the sequences of the rules.</p> <p>See Create an AP Power Profile, on page 262.</p>
Support for Custom AP Profiles	<p>AP profiles consolidate the AP authentication settings, aWIPS, rogue management, and mesh settings. AP profiles allow you to manage and provision APs.</p> <p>Cisco DNA Center provides a default AP profile for Cisco IOS XE devices and Cisco AireOS devices. You can create custom AP profiles for Cisco IOS XE devices and Cisco AireOS devices.</p> <p>Note If there are any out-of-band custom AP profiles that are created directly on the wireless controller and used with Cisco DNA Center running earlier than Release 2.3.5, ensure that you create a custom AP profile on Cisco DNA Center with same name and map it to the custom site tag to retain the configuration.</p> <p>See AP Profiles, on page 253, Create an AP Profile for Cisco IOS XE Devices, on page 254, Create an AP Profile for Cisco AireOS Devices, on page 260, Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 285, and About Wireless Mesh Networks, on page 271.</p>
Support for Native Multicast over SD-Access Transit	<p>You can configure SD-Access Native Multicast on a network that has multiple fabric sites that are connected to an SD-Access transit. Cisco DNA Center provides an option to enable multicast on the border nodes and on the SD-Access transit.</p> <p>See Add a Device as a Border Node, on page 476 and Create an SD-Access Transit, on page 480.</p>
Support for Reuse of AP Groups and Flex Groups Within an Area	<p>While creating a network profile for wireless, you can use the same AP group and flex group across sites (buildings or floors) within an area.</p> <p>See Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 285.</p>

Feature	Description
Support for Wireless IP Address Pools from Layer 2 Segments for Cisco SD-Access Fabric Sites	<p>You can choose the wireless IP address pools that are configured for Layer 2 segments while configuring wireless SSIDs for fabric sites.</p> <p>See Configure Wireless SSIDs for Fabric Networks, on page 483.</p>
Support Multiple IPv4 Addresses on Single Wired MAC Address in a Cisco SD-Access Fabric	<p>You can connect wired endpoints with multiple IPv4 addresses to a Cisco SD-Access fabric.</p> <p>See Create Anycast Gateways, on page 487.</p>
Template Hub	<p>You can filter CLI templates based on Project Name, Template Language, Device Family, Device Series, Commit State, and Provision Status from Tools > Template Hub.</p> <p>You can attach the CLI template to network profiles in the Template Hub window. You can also create a new network profile.</p> <p>See About Template Hub, on page 291 and Attach a CLI Template to the Network Profiles, on page 300.</p>



PART I

Get Started

- [Get Started with Cisco DNA Center, on page 11](#)
- [Configure Telemetry, on page 27](#)



CHAPTER 2

Get Started with Cisco DNA Center

- [Cisco DNA Center Overview, on page 11](#)
- [Log In, on page 11](#)
- [Complete the Quick Start Workflow, on page 12](#)
- [User Profile Roles and Permissions, on page 17](#)
- [Default Home Page, on page 17](#)
- [Cisco DNA Center Journey Map, on page 21](#)
- [View the Remote Support Authorization Dashboard, on page 22](#)
- [Use Global Search, on page 23](#)
- [Enable Localization, on page 25](#)
- [Subscribe to Cisco DNA Center Insights, on page 26](#)

Cisco DNA Center Overview

Cisco Digital Network Architecture offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center GUI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

Log In

Access Cisco DNA Center by entering its network IP address in your browser. For compatible browsers, see the [Cisco DNA Center Release Notes](#). This IP address connects to the external network and is configured during the Cisco DNA Center installation. For more information about installing and configuring Cisco DNA Center, see the [Cisco DNA Center Installation Guide](#).

You should continuously use Cisco DNA Center to remain logged in. If you are inactive for too long, Cisco DNA Center logs you out of your session automatically.

Step 1 Enter an address in your web browser's address bar in the following format. Here, *server-ip* is the IP address (or the hostname) of the server on which you have installed Cisco DNA Center:

`https://server-ip`

Example: `https://192.0.2.1`

Depending on your network configuration, you might have to update your browser to trust the Cisco DNA Center server security certificate. Doing so will help ensure the security of the connection between your client and Cisco DNA Center.

Step 2 Enter the Cisco DNA Center username and password assigned to you by the system administrator. Cisco DNA Center displays its home page.

If your user ID has the SUPER-ADMIN-ROLE and no other user with the same role has logged in before, you will see a first-time setup wizard instead of the home page.

Step 3 To log out, click the menu icon (☰) and choose **Sign Out**.

Complete the Quick Start Workflow

After you have installed and configured the Cisco DNA Center appliance, you can log in to its GUI. Use a compatible, HTTPS-enabled browser when accessing Cisco DNA Center.

When you log in for the first time as the admin superuser (with the username `admin` and the SUPER-ADMIN-ROLE assigned), the Quick Start workflow automatically starts. Complete this workflow to discover the devices that Cisco DNA Center will manage and enable the collection of telemetry from those devices.

Before you begin

To log in to Cisco DNA Center and complete the Quick Start workflow, you will need:

- The `admin` superuser username and password that you specified while completing one of the following procedures in the [Cisco DNA Center Second-Generation Appliance Installation Guide](#):
 - Configure the Primary Node Using the Maglev Wizard
 - Configure an Appliance Using the Install Configuration Wizard (44- or 56-core appliance)
 - Configure an Appliance Using the Install Configuration Wizard (112-core appliance)
 - Configure the Primary Node Using the Advanced Install Configuration Wizard (44- or 56-core appliance)
 - Configure the Primary Node Using the Advanced Install Configuration Wizard (112-core appliance)
- The information described in the installation guide's Required First-Time Setup Information topic.

Step 1 After the Cisco DNA Center appliance reboot is completed, launch your browser.

Step 2 Enter the host IP address to access the Cisco DNA Center GUI, using **HTTPS://** and the IP address of the Cisco DNA Center GUI that was displayed at the end of the configuration process.

After entering the IP address, one of the following messages is displayed (depending on the browser you are using):

- Google Chrome: `Your connection is not private`
- Mozilla Firefox: `Warning: Potential Security Risk Ahead`

Step 3 Ignore the message and click **Advanced**.

One of the following messages is displayed:

- **Google Chrome:**

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
```

- **Mozilla Firefox:**

```
Someone could be trying to impersonate the site and you should not continue. Websites prove their identity via certificates. Firefox does not trust GUI-IP-address because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.
```

These messages are displayed because the controller uses a self-signed certificate. For information on how Cisco DNA Center uses certificates, see the "Certificate and Private Key Support" section in the [Cisco DNA Center Administrator Guide](#).

Step 4 Ignore the message and do one of the following:

- Google Chrome: Click the **Proceed to GUI-IP-address (unsafe)** link.
- Mozilla Firefox: Click **Accept the Risk and Continue**.

The Cisco DNA Center login window opens.

Step 5 Do one of the following and then click **Log In**:

- If you completed the Maglev configuration wizard and chose the **Start using DNAC pre manufactured cluster** option, enter the admin's username (**admin**) and password (**maglev1@3**).
- If you completed the Maglev configuration wizard and chose the **Start configuration of DNAC in advanced mode** option, enter the admin's username (**admin**) and password that you set when you configured your Cisco DNA Center appliance.
- If you completed the Install configuration wizard, enter the admin's username (**admin**) and paste the password (**maglev1@3**) that you copied from the wizard's final window.
- If you completed the Advanced Install configuration wizard, enter the admin's username (**admin**) and password that you set when you configured your Cisco DNA Center appliance.

In the next window, you are prompted to specify a new admin password (as a security measure).

Step 6 Do one of the following:

- If you don't want to change the admin password at this time, click **Skip**.
- To set a new admin password:
 - a. Enter the same password that you specified in Step 5.
 - b. Enter and confirm a new admin password.
 - c. Click **Next**.

Step 7 Enter your cisco.com username and password (which are used to register software downloads and receive system communications) and then click **Next**.

Note If you don't want to enter these credentials at this time, click **Skip** instead.

The **Terms & Conditions** window opens, providing links to the software End User License Agreement (EULA) and any supplemental terms that are currently available.

Step 8 After reviewing these documents, click **Next** to accept the EULA.

The **Quick Start Overview** slider opens. Click > to view a description of the tasks that the Quick Start workflow will help you complete in order to start using Cisco DNA Center.

Step 9 Complete the Quick Start workflow:

a) Click **Let's Do it**.

b) In the **Discover Devices: Provide IP Ranges** window, enter the following information and then click **Next**:

- The name for the device Discovery job.
- The IP address ranges of the devices you want to discover. Click + to enter additional ranges.
- Specify whether you want to designate your appliance's loopback address as its preferred management IP address. For more information, see the "Preferred Management IP Address" topic in the [Cisco DNA Center User Guide](#).

c) In the **Discover Devices: Provide Credentials** window, enter the information described in the following table for the type of credentials you want to configure and then click **Next**:

Field	Description
CLI (SSH) Credentials	
Username	Username used to log in to the CLI of the devices in your network.
Password	Password used to log in to the CLI of the devices in your network. The password you enter must be at least eight characters long.
Name/Description	Name or description of the CLI credentials.
Enable Password	Password used to enable a higher privilege level in the CLI. Configure this password only if your network devices require it.
SNMP Credentials: SNMPv2c Read tab	
Note	Cisco DNA Center does not support SNMPv2c credentials when FIPS mode is enabled. You'll need to enter SNMPv3 credentials instead. For more information about FIPS mode, see the "Configure the Primary Node Using the Maglev Wizard" topic in the Cisco DNA Center Second-Generation Appliance Installation Guide .
Name/Description	Name or description of the SNMPv2c read community string.
Community String	Read-only community string password used only to view SNMP information on the device.
SNMP Credentials: SNMPv2c Write tab	
Name/Description	Name or description of the SNMPv2c write community string.
Community String	Write community string used to make changes to the SNMP information on the device.
SNMP Credentials: SNMPv3	

Field	Description
Name/Description	Name or description of the SNMPv3 credentials.
Username	Username associated with the SNMPv3 credentials.
Mode	<p>Security level that SNMP messages require:</p> <ul style="list-style-type: none"> • No Authentication, No Privacy (noAuthnoPriv): Does not provide authentication or encryption. • Authentication, No Privacy (authNoPriv): Provides authentication, but does not provide encryption. • Authentication and Privacy (authPriv): Provides both authentication and encryption. <p>Note When FIPS mode is enabled, Cisco DNA Center only supports Authentication and Privacy mode.</p>
Authentication Password	<p>Password required to gain access to information from devices that use SNMPv3. The password must be at least eight characters in length. Note the following points:</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Authentication Type	<p>Hash-based Message Authentication Code (HMAC) type used when either Authentication and Privacy or Authentication, No Privacy is set as the authentication mode:</p> <ul style="list-style-type: none"> • SHA: HMAC-SHA authentication. • MD5: HMAC-MD5 authentication. <p>Note Cisco DNA Center does not support this authentication type when FIPS mode is enabled.</p>
Privacy Type	<p>Privacy type. (Enabled if you select Authentication and Privacy as Mode.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages are exchanged with devices supported with AES128, AES192, and AES256 encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note the following points:</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
NETCONF	
Port	The NETCONF port that Cisco DNA Center should use in order to discover wireless controllers that run Cisco IOS-XE.

- d) In the **Create Site** window, group the devices you are going to discover into one site in order to facilitate telemetry and then click **Next**.

You can enter the site's information manually or click the location you want to use in the provided map.

- e) In the **Enable Telemetry** window, check the network components that you want Cisco DNA Center to collect telemetry for and then click **Next**.

Note If both the **Enable Telemetry** and **Disable Telemetry** options are grayed out, this indicates that either devices are not capable of supporting telemetry or devices are running an OS version that does not support telemetry enablement.

- f) In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

- If you're happy with the settings, click **Start Discovery and Telemetry**. Cisco DNA Center validates your settings to ensure that they will not result in any issues. After validation is complete, the window updates.

Cisco DNA Center begins the process of discovering your network's devices and enabling telemetry for the network components you selected. The process will take a minimum of 30 minutes (more for larger networks).

A message is displayed at the top of the homepage to indicate when the Quick Start workflow has completed.

- g) Do one of the following:

- Click **View Discovery** to open the **Discovery** window and confirm that the devices in your network have been discovered.
- Click the **Go to Network Settings** link to open the **Device Credentials** window. From here, you can verify that the credentials you entered previously have been configured for your site.
- Click the **View Activity Page** link to open the **Tasks** window and view any tasks (such as a weekly scan of the network for security advisories) that Cisco DNA Center has already scheduled to run.
- Click the **Workflow Home** link to access guided workflows that will help you set up and maintain your network.

User Profile Roles and Permissions

Cisco DNA Center supports role-based access control (RBAC). The roles assigned to a user profile define the capabilities that a user has permission to perform. Cisco DNA Center has three main default user roles:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- OBSERVER-ROLE

The SUPER-ADMIN-ROLE gives users broad capabilities and permits them to perform all actions in the Cisco DNA Center GUI, including creating custom roles and assigning them to user profiles. The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE have more limited and restricted capabilities in the Cisco DNA Center GUI.

If you're unable to perform an action in Cisco DNA Center, the reason might be that your user profile is assigned a role that doesn't permit it. For more information, check with your system administrator or see the [Cisco DNA Center Administrator Guide](#).

Default Home Page

After you log in, Cisco DNA Center displays its home page. The home page has the following main areas: **Assurance Summary**, **Network Snapshot**, **Network Configuration**, and **Tools**.



Note By default, the login name you provided is displayed in the Welcome text. To change the name, click the name link; for example, **admin**. You are taken to the **User Management** window, where you can edit the display name.

Assurance Summary

This area includes:

- **Health**: Provides the health score of your overall enterprise, which includes network devices, wired clients, and wireless clients. Clicking **View Details** takes you to the **Overall Health** window.
- **Critical Issues**: Provides the count of P1 and P2 issues. Clicking **View Details** takes you to the **Open Issues** window.
 - **P1**: Critical issues that need immediate attention before they cause a wider impact on network operations.
 - **P2**: Major issues that can potentially impact multiple devices or clients.
- **Trends and Insights**: Provides insights about the performance of your network. Clicking **View Details** takes you to the **Network Insights** window.

Network Snapshot

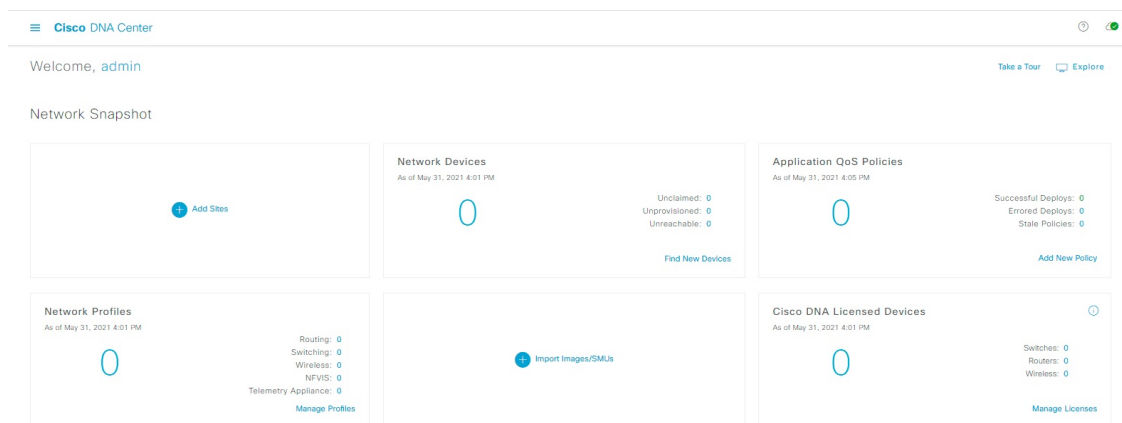
This area includes:

- **Sites:** Provides the number of sites discovered on your network along with the number of DNS and NTP servers. Clicking **Add Sites** takes you to the **Add Site** window.
- **Network Devices:** Provides the number of network devices discovered on your network along with the number of unclaimed, unprovisioned, and unreachable devices. Clicking **Find New Devices** takes you to the **New Discovery** window.
- **Application Policies:** Provides the number of application policies discovered on your network along with the number of successful and errored deployments. Clicking **Add New Policy** takes you to the **Application Policies** window.
- **Network Profiles:** Provides the number of profiles discovered on your network. Clicking **Manage Profiles** takes you to the **Network Profiles** window.
- **Images:** Provides the number of images discovered on your network along with the number of untagged and unverified images. Clicking **Import Images/SMUs** takes you to the **Image Repository** window.
- **Licensed Devices:** Provides the number of devices that have a Cisco DNA Center license along with the number of switches, routers, and access points. Clicking **Manage Licenses** takes you to the **License Management** window.
- **EoX Status:** Provides the number of devices scanned and EoX alerts discovered on your network. Clicking **Accept Cisco CX Cloud EULA** takes you to the **CX Cloud platform** window. Read the information in the **Accept Cisco CX Cloud EULA** window and click **OK** to scan the network for EoX alerts.

Tools

Use the **Tools** area to configure and manage your network.

Figure 1: Cisco DNA Center Home Page



Different Views of Home Page

The home page can vary depending factors such as the different stages of Cisco DNA Center and what role is used to log in:

- **Getting Started:** When you log in to Cisco DNA Center for the first time as a Network Administrator or System Administrator, or when there are no devices in the system, you see the following dashlet. Click **Get Started** and complete the getting started workflow to discover new devices in your network.

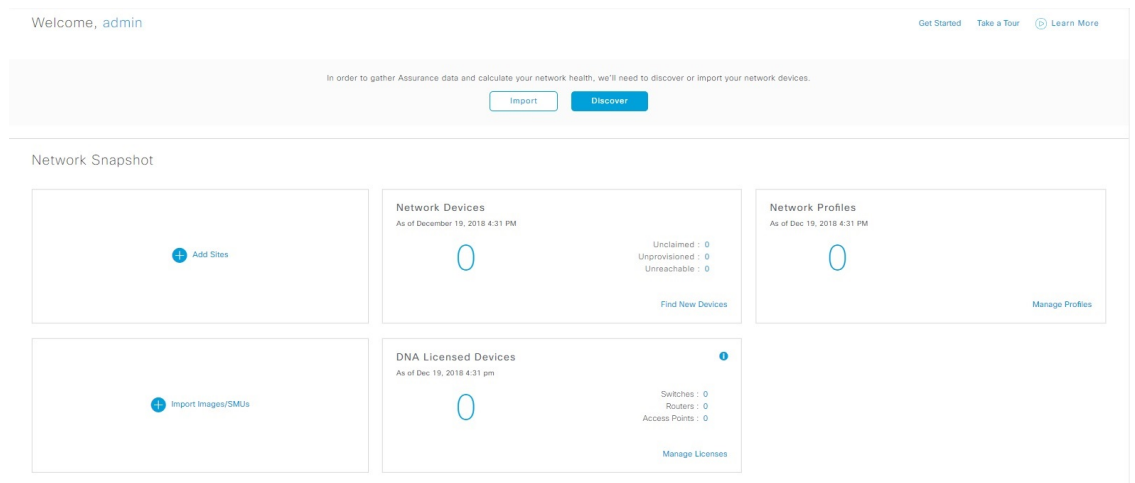
In a few simple steps, discover your devices to begin your Cisco DNA Center journey!

Get Started

When you log in to Cisco DNA Center for the first time as an Observer, you see the following message:

Ask your Network Administrator to add Network Devices to gather Assurance data.

- **Day 0 Home Page:** If you skipped getting started, or when there are no devices in the system, you see the following home page.



When discovery is in progress, you see a progress message with a link to the **Discovery** window.

We've discovered 10 devices in your network. [View Discovery](#)

When there are devices in the system, you see a network snapshot of discovered devices.




Menu Bar

Click the menu icon (☰) at the left of the menu bar to access the menu items.

Icons

Click the icons at the right of the menu bar to perform common tasks:

Icon	Description
🔍	Search: Search for devices, users, hosts, menus, and other items that are stored anywhere in the Cisco DNA Center database.

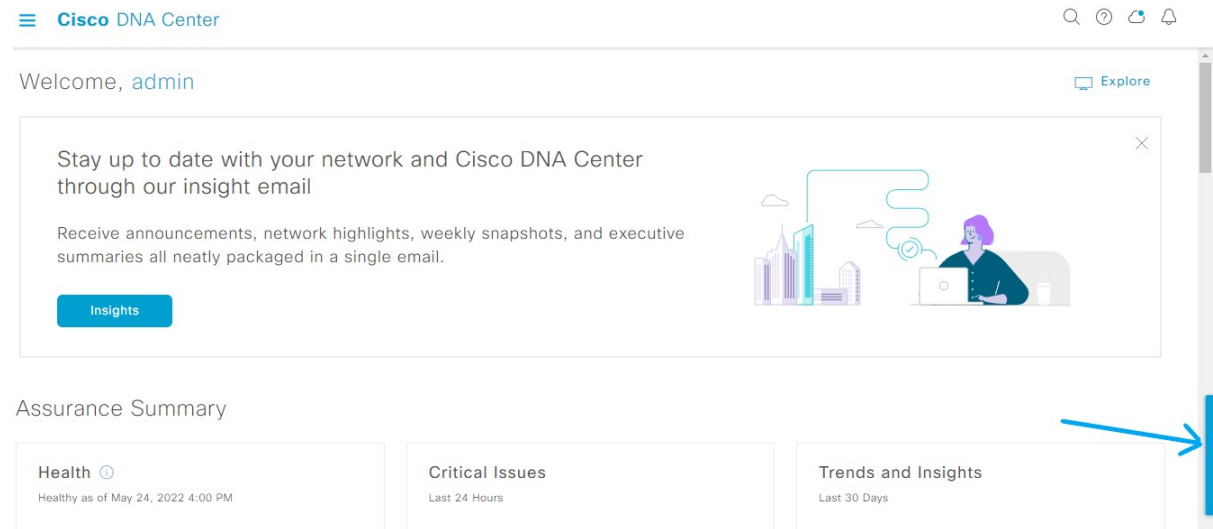
Icon	Description
	<p>Help</p> <ul style="list-style-type: none"> • About: Display the current Cisco DNA Center software version. Click Release Notes to launch the release notes in a separate browser tab. Click Packages to view the system and application package versions. Click Serial number to view the serial number of the Cisco DNA Center appliance. • API Reference: Open the Cisco DNA Center platform API documentation in Cisco DevNet. • Developer Resources: Open Cisco DevNet, where you can access developer tools. • Contact Support: Open a support case with the Cisco Technical Assistance Center (TAC). • Remote Support Authorization: Grant remote access to a Cisco specialist to access Cisco DNA Center for troubleshooting your network. For more information, see View the Remote Support Authorization Dashboard, on page 22. • Help: Launch context-sensitive online help in a separate browser tab. • Cisco CX Cloud Success Tracks: Allows you to access the Cisco CX cloud success tracks website in a new window. • Keyboard Shortcuts: Display the keyboard shortcut names, shortcut keys, and shortcut key combinations for shortcut groups. The supported shortcut groups are Global, Geo Maps, and Topology. • Make a Wish: Submit your comments and suggestions to the Cisco DNA Center product team.
	<p>Software Updates: See a list of available software updates. Click the Go to Software Updates link to view system and application updates.</p>
	<p>Notifications: View event notifications and set notification preferences. A red circle by the notification icon indicates that there are new notifications.</p>

Interactive Help

Interactive Help contains walkthroughs for specific tasks in Cisco DNA Center. The walkthroughs provide onscreen guidance to help you complete the task.

The **Interactive Help** widget is displayed by default at the bottom-right corner of the Cisco DNA Center window. Click the widget to open the **Interactive Help** menu.

Figure 2: Interactive Help Widget



You can also move the **Interactive Help** widget from the default location to other locations. Drag and drop the widget to the possible locations, which are indicated by green dotted-line rectangles.

Cisco DNA Center Journey Map

The Cisco DNA Center journey map shows various capabilities provided by Cisco DNA Center and its usage.

To launch the Cisco DNA Center journey map, do any one of the following:

- Click the menu icon (☰) and choose **Explore**.
- In the Cisco DNA Center home page, click **Begin Your Journey**.

In the Cisco DNA Center journey map, the various features (capabilities) provided by Cisco DNA Center are grouped into the following tabs: AIOps, NetOps, DevOps, and SecOps. Each tab shows the features in a doughnut chart. The features are further grouped into segments in the doughnut chart.

Hover your mouse over the features displayed in the doughnut chart to view a brief description about the feature and the status. Click the feature displayed in the doughnut chart to open the feature window.

From the **Filter By** drop-down list, choose the following options to view the features in a specific state:

- Successfully Completed
- Active
- Inactive
- Not available

View the Remote Support Authorization Dashboard

Remote support authorization allows you to grant remote access to a Cisco specialist to access Cisco DNA Center and troubleshoot your network.



Note The Cisco DNA Center remote support authorization is supported only with RADKit version 1.2.1 or later.

Step 1 In the Cisco DNA Center GUI, click the help icon in the top-right corner and choose **Remote Support Authorization**. In the **Remote Support Authorization** dashboard, the **SUMMARY** area shows the total, scheduled, and completed remote support authorizations.

Step 2 Click the **Create New Authorization** tab to create a new authorization. For more information, see [Create a Remote Support Authorization, on page 731](#).

Step 3 Click the **Current Authorization** tab to view the current remote support authorization tiles with the following possible status:

- **All:** Displays all the scheduled and active remote support authorizations.
- **Scheduled:** Displays the scheduled remote support authorizations.
- **Active:** Displays the active remote support authorizations.

The support authorization tile shows the schedule and duration of Cisco specialist access to Cisco DNA Center for troubleshooting purposes.

Step 4 To cancel an authorization, click the **Cancel Authorization** link in the respective support authorization tile.

Step 5 Click **View Logs** to navigate to the **Audit Logs** window, which lists the remote support authorization logs.

For more information, see **View Audit Logs** in the [Cisco DNA Center Administrator Guide](#).

Step 6 Click the **Past Authorizations** tab to view the past authorizations.

The **Past Authorizations** table shows the support authorization based on **Cisco Specialist**, **Happened On**, **Session Status**, and **Log** and lists the following past authorizations status:

- **All:** Lists all the expired and canceled remote support authorizations.
- **Expired:** Lists all the expired remote support authorizations.
- **Canceled:** Lists all the canceled remote support authorizations.

Step 7 Click **Manage SSH Credentials** to establish the SSH connection to Cisco DNA Center. For more information, see [Configure SSH Credentials, on page 23](#).

- Note**
- The number of nodes in the deployment determines the maximum number of SSH credentials.
 - SSH credentials only need to be created once if all nodes use the same password.

In the **Remote Support Authorization** dashboard, the Remote Support Cloud service connectivity status is shown:

- A green check mark in the top-right corner indicates that the remote support authorization is connected to the Remote Support Cloud service.
 - An exclamation point in the top-right corner indicates that the remote support authorization is not connected to the Remote Support Cloud service.
-

Configure SSH Credentials

SSH credentials allow a Cisco specialist to access your Cisco DNA Center setup for troubleshooting.


- Step 1** Click the menu icon (☰) and choose **Remote Support Authorization > Manage SSH Credential > Add New SSH Credentials**.
- Step 2** In the **Add New SSH Credentials** slide-in pane, do the following:
- a. In the **Password** field, enter a password.
 - b. In the **Name/Description** field, enter a name or description to identify the password.
- Step 3** Click **Add**.
- Note**
- The number of nodes in the deployment determines the maximum number of SSH credentials.
 - SSH credentials only need to be created once if all nodes use the same password.
 - When you reach the maximum number of SSH credentials, you must delete an existing credential before you can add a new one.
- Step 4** To edit an SSH credential, do the following:
- a. In the **Existing SSH Credentials** area, click **Edit**.
 - b. In the **Edit SSH Credentials** slide-in pane, make your changes and click **Save**.
- Step 5** To delete an SSH credential, do the following:
- a. In the **Existing SSH Credentials** area, click **Delete**.
 - b. In the confirmation window, click **Confirm**.
-

Use Global Search

Use the global Search function to find items in the following categories anywhere in Cisco DNA Center:

- **Activities:** Search for Cisco DNA Center menu items, workflows, and features by name.
- **Applications:** Search for them by name.

- **Application Groups:** Search for them by name.
- **Authentication template:** Search for them by name or type.
- **Devices:** Search for them by collection status, reachability status, location, or tag.
- **Fabric:** Search by fabric name.
- **Help:** Search for topics that include your search string.
- **Hosts and Endpoints:** Search for them by name, IP address, or MAC address.
- **IP Pools:** Search for them by name or IP address.
- **Network Devices:** Search for them by name, IP address, serial number, software version, platform, product family, or MAC address.
- **Network Profiles:** Search by profile name.
- **Network Settings**
 - **Device Credentials:** Search by name.
 - **IP Address Pools:** Search for them by group name or pool CIDR.
 - **Service Provider Profiles:** Search for them by profile name, WAN provider, or model.
- **Policy:** Search for them by name or description.
- **Sites:** Search for them by name.
- **Traffic copy:** Search for them by name and description.
- **Transits:** Search by transit name.
- **Users:** Search for the system settings and users by username. Case-insensitivity and substring search are not supported for usernames.
- Other items, as new versions of Cisco DNA Center are released.

To start a global Search, click the  icon in the top-right corner of any Cisco DNA Center window. Cisco DNA Center displays a global search window, with a Search field where you can begin entering identifying information about an item.

You can enter all or part of the item's name, address, serial number, or other identifying information. The Search field is case-insensitive and can contain any character or combination of characters.

As you begin entering your search string, Cisco DNA Center displays a list of possible search targets that match your entry. If more than one category of item matches your search string, Cisco DNA Center sorts them by category, with a maximum of five items in each category. The first item in the first category is selected automatically, and summary information for that item is displayed in the summary panel on the right.

You can scroll the list as needed, and click any of the suggested search targets to see information for that item in the summary panel. If there are more than five items in a category, click **View All** next to the category name. To return to the categorized list from the complete list of search targets, click **Go Back**.

As you add more characters to the search string, global Search automatically narrows the displayed list.

Cisco DNA Center allows you to search for a device using its entire IPv6 address or any abbreviated form of the IPv6 address.

For example, to search for `2001:0db8:85a3:0000:0000:8a2e:0370:7334`, you can use the following search entries:


- `2001:0db8:85a3:0000:0000:8a2e:0370:7334` (using the full IPv6 address)
- `2001:db8:85a3:0:0:8a2e:0:7334` (truncating leading zeros)
- `2001:db8:85a3::8a2e:0:7334` (compressing consecutive zeros with a double colon)
- `2001:db8:85a3` (using a portion of the IPv6 address)

Cisco DNA Center allows you to search for an IPv6 address by using the double colon in the IPv6 address with prefix, postfix, or any combination.

For example, to search for `2001:db8:85a3::8a2e:0:7334`, you can use the following search entries:

- `::` (using double colon alone)
- `85a3::8a2e` (using prefix and postfix with double colon)
- `85a3::` (using prefix with double colon)
- `::8a2e` (using postfix with double colon)

You can search for devices in Cisco DNA Center by entering their MAC addresses in any format (with a hyphen or colon).

When you are finished, click  to close the window.



Global search can display five results per category at a time.

Enable Localization

You can view the Cisco DNA Center GUI windows in English (the default), Chinese, Japanese, or Korean.

To change the default language, perform the following task:

Step 1 In your browser, change the locale to one of the supported languages: Chinese, Japanese, or Korean.

- From Google Chrome, do the following:
 - a. Click the  icon in the top-right corner, and then choose **Settings**.
 - b. Click **Languages**.
 - c. Click **Add languages**.
 - d. In the **Add languages** dialog box, choose **Chinese**, **Japanese**, or **Korean**, and then click **Add**.
- From Mozilla Firefox, do the following:
 - a. Click the  icon in the top-right corner, and then choose **Settings**.

- b. From the **Language and Appearance > Language** area, click **Choose**.
- c. From the **Select a language to add** drop-down list, choose **Chinese, Japanese, or Korean**.
- d. Click **OK**.

Step 2 Log in to Cisco DNA Center.

The GUI is shown in the selected language.

Subscribe to Cisco DNA Center Insights

You can subscribe to the *Cisco DNA Center Insights* publication, which contains product announcements, network highlights, information about your network performance, and more. *Cisco DNA Center Insights* is sent in PDF format to the email address that you specify.



Note If your Cisco DNA Center appliance is deployed in a secure, air-gapped network, certain metrics are omitted from *Cisco DNA Center Insights*. To view the complete *Cisco DNA Center Insights*, you must have internet and telemetry connectivity, which aren't available in air-gapped environments.

Before you begin

- Under **System > Settings > Integration Settings**, enter your callback URL hostname or IP address. For more information, see "Configure Integration Settings" in the [Cisco DNA Center Administrator Guide](#).
- Under **System > Settings > External Services > Destinations > Email**, configure the SMTP servers that you will use to receive the publication.

Step 1 Click the menu icon (≡), hover your cursor over your displayed username, and choose **My Profile and Settings > Communication Preferences**.

Step 2 Click the **Subscription Off** toggle to enable the **Subscription On** option.

Step 3 Enter the email address at which you want to receive *Cisco DNA Center Insights*, and click **Save**.

Insights are archived for up to one year. You can read past publications by choosing **Actions > Download PDF** for the corresponding date range.

Step 4 (Optional) To change the email address, click the pencil icon.

Step 5 (Optional) To unsubscribe from *Cisco DNA Center Insights*, click the **Subscription On** toggle to enable the **Off** option.



CHAPTER 3

Configure Telemetry

- [Application Telemetry Overview](#), on page 27
- [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry](#), on page 27
- [Criteria for Enabling Application Telemetry on Devices](#), on page 28
- [Provision Application Telemetry Settings](#), on page 30
- [Enable Application Telemetry for Wireless Controllers](#), on page 31
- [Update Telemetry Settings to Use a New Cluster Virtual IP Address](#), on page 32
- [Update Device Configuration Using Telemetry](#), on page 33

Application Telemetry Overview

Application telemetry allows you to configure global network settings on devices for monitoring and assessing their health.

Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry

With Cisco DNA Center, you can configure global network settings when devices are assigned to a specific site. Telemetry polls network devices and collects telemetry data according to the settings in the SNMP server, syslog server, NetFlow Collector, or wired client.

Before you begin

Create a site and assign a device to the site. See [Create, Edit and Delete a Site](#), on page 134.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > Telemetry**.

Step 2 In the **SNMP Traps** area, do one of the following:

- Check the **Use Cisco DNA Center as SNMP trap server** check box.
- Check the **Add an external SNMP trap server** check box and enter the IP address of the external SNMP trap server. The selected server collects SNMP traps and messages from the network devices.

Step 3 In the **Syslogs** area, do one of the following:

- Check the **Use Cisco DNA Center as syslog server** check box.
- Check the **Add an external syslog server** check box and enter the IP address of the external syslog server.

Step 4 In the **NetFlow** area, do one of the following:

- Click the **Use Cisco DNA Center as NetFlow collector server** radio button. The NetFlow configuration on the device interfaces is completed only when you enable application telemetry on the device. Select the NetFlow collector at the site level to configure the NetFlow destination server to the device.
- Click the **Add Cisco Telemetry Broker (CTB)** radio button and add the IP address and port number of the Cisco Telemetry Broker. The Cisco Telemetry Broker collects NetFlow records from the device and sends the information to the destination.

Note Cisco DNA Center must be configured as a destination in Cisco Telemetry Broker to receive NetFlow records. If Cisco DNA Center is not configured as a destination, the Application Experience does not work.

Step 5 In the **Wired Endpoint Data Collection** area, click the **Enable Cisco DNA Center Wired Endpoint Data Collection At This Site** radio button to turn on IP Device Tracking (IPDT) on the access devices of the site.

If you don't want to enable IPDT for the site, click the **Disable** radio button (the default).

Note You must enable IPDT to preview the CLI configuration. When provisioning a device, you can preview the CLI configuration before deploying it on the device.

Step 6 In the **Wireless Controller, Access Point and Wireless Clients Health** area, check the **Enable Wireless Telemetry** check box to monitor the health of the wireless controllers, APs, and wireless clients in your network.

Step 7 Click **Save**.

Criteria for Enabling Application Telemetry on Devices

Cisco DNA Center automatically enables application telemetry on all applicable interfaces or WLANs that are selected based on the new automatic interfaces or WLAN selection algorithm.

Application telemetry is pushed to WLANs that are provisioned through Cisco DNA Center.



Note

- The conventional tagging-based algorithm is supported and has precedence over the newer automatic interfaces or WLAN selection algorithm.
- If you want to switch over from the automatic selection algorithm to the tagging-based algorithm, you must disable telemetry before provisioning the tagged SSIDs to the devices.

The following table provides the criteria for selecting interfaces and WLANs based on the conventional tagging-based algorithm (with **lan** keyword) and the new automatic selection algorithm for all the supported platforms:

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm
Router	<ul style="list-style-type: none"> • Interface description has the lan keyword.^{1,2} • Interface has an IP address other than the management IP address. 	<ul style="list-style-type: none"> • Interface has an IP address other than the management IP address. • Interface is not any of the following: <ul style="list-style-type: none"> • WAN <p>Note An interface is treated as a WAN-facing interface if it has a public IP address, and if there is a route rule with a public IP address that routes through the interface.</p> <p>In this context, a public IP address is not in a private range (for example, not in 192.168.x.x, 172.16.y.y, 10.z.z.z), or is an IP address that is not in the system's IP pools.</p> <p>Route rules can be dynamically learned. In this context, the show ip route command does not show a route to a public IP address that goes through this interface.</p> • Loopback. • Management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, or FASTETHERNET1.
Switch	<ul style="list-style-type: none"> • Interface description has the lan keyword.^{1,2} • Switch port is configured as an access port. • Switch port is configured with the switch-mode access command. 	<ul style="list-style-type: none"> • Interface is a physical interface. • Access port does not have neighbors. • Interface is not any of the following: <ul style="list-style-type: none"> • Management interface: FASTETHERNET0, FASTETHERNET1, GIGABITETHERNET0/0, or MGMT0 • LOOPBACK0, Bluetooth, App Gigabit, WPAN, Cellular, or Async • VSL interface.


Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm
Cisco AireOS Controller	WLAN profile name is tagged with the lan keyword. ^{1,2}	If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, Wireless Service Assurance (WSA) processing is enabled. If all the SSIDs are in Local mode, NetFlow is enabled.
Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS 16.12.1 and later.	WLAN profile name is tagged with the lan keyword. ^{1,2}	If the SSIDs are mixed—that is, central switching, Flex mode, and Fabric mode—the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs use central switching, the Optimized APM record is configured. For Cisco Catalyst 9800 Series Wireless Controllers with IOS 17.10 and later, Cisco DNA Center pushes the APM profile, not the AVC basic profile, for flex and fabric SSIDs.
	Note If you want to update the telemetry configuration, you must disable telemetry and then enable it after making the configuration changes.	
Cisco DNA Traffic Telemetry Appliance with Optimized APM profile and IOS 17.3 and later.	<ul style="list-style-type: none"> Interface description has the lan keyword.^{1,2} Interface is a physical interface. 	<ul style="list-style-type: none"> Interface is a physical interface. Interface is not a management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, and FASTETHERNET1.

¹ The **lan** keyword is case insensitive and can be separated by a space, hyphen, or underscore.

² Resynchronize the network device to read the **lan** interface description.

Provision Application Telemetry Settings

Configure global telemetry settings as described in [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 27](#).

Step 1 Click the menu icon () and choose **Provision > Network Devices > Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the Global site in the left pane and select the site, building, or floor.

Step 2 Choose the devices that you want to provision.

Step 3 From the **Actions** drop-down list, choose **Telemetry** and do one of the following:

Note The application telemetry option is enabled only if the device supports application telemetry enablement from Cisco DNA Center.

a) **Enable Application Telemetry**: To configure application telemetry for the selected devices.

b) **Disable Application Telemetry**: To remove the application telemetry configuration from the chosen devices.

Step 4 Click **Apply**.

The **Application Telemetry** column shows the telemetry configuration status. If you don't see the **Application Telemetry** column in the default column setting, click the ellipsis icon (⋮) at the right end of the column headings and check the **Application Telemetry** check box.

Enable Application Telemetry for Wireless Controllers

You can enable application telemetry for new and existing devices.

Before you begin

To enable application telemetry, devices must have a Cisco DNA Advantage license.



Note Before enabling application telemetry in Cisco DNA Center, ensure to delete any existing flow monitors configured manually from **Configuration > Services > Application Visibility > Flow Monitors** through the Cisco Catalyst 9800 Series Wireless Controller GUI.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 2** To view devices available in a particular site, expand the **Global** site in the left pane, and choose the site, building, or floor.
- Step 3** In the **Inventory** window, choose the device. You can choose multiple devices at a time.
- Step 4** From the **Action** drop-down list choose **Telemetry > Enable Application Telemetry**.
- Step 5** In the **Enable Telemetry** slide-in pane, complete the following settings:
- AP mode: Check the **Flex/Fabric** or **Local** check box. You can also choose both options.
 - Check the **Include Guest SSID** check box to enable telemetry for guest SSIDs.
 - Telemetry Source:**
 - Embedded Wireless Controllers - NetFlow
 - AireOS wireless controller (Local mode) - NetFlow
 - AireOS wireless controller (Flex/Fabric mode) - Wireless Service Assurance (WSA)
 - To apply the same settings for all wireless controllers, check **Apply this selection to all wireless controllers**.
- Step 6** Click **Enable**.
- Step 7** In the **Application Telemetry** window, click **ok**.
- To skip this screen in the future, check **Don't show again**.
- The telemetry status is shown in the **Application Telemetry** column in the **Inventory** window.
-

Update Telemetry Settings to Use a New Cluster Virtual IP Address

If you are using the Cisco DNA Center application telemetry to monitor device data, and you need to change the Cisco DNA Center cluster virtual IP address (VIP), complete the following steps to change the VIP and to ensure that node telemetry data is sent to the new VIP.

Before you begin

- Determine the version of Cisco DNA Center that you are using. You can check this by logging in to the Cisco DNA Center GUI and using the **About** option to view the Cisco DNA Center version number.
- Obtain SSH client software.
- Identify the VIP address that was configured for the 10-GB interface facing the enterprise network on the Cisco DNA Center primary node. Log in to the appliance using this address, on port 2222. To identify this port, see the rear-panel figure in the "Front and Rear Panels" section in the [Cisco DNA Center Installation Guide](#).
- Obtain the Linux username (**maglev**) and password configured on the primary node.
- Identify the cluster VIP that you want to assign. The cluster VIP must conform to the requirements explained in the "Required IP Addresses and Subnets" section in the [Cisco DNA Center Installation Guide](#).

Step 1 Access the Cisco DNA Center GUI and disable Application Telemetry at all the sites, as follows:

- Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the Global site in the left pane, and select the site, building, or floor.

- Choose all the sites and devices currently being monitored.
- From the **Actions** drop-down list, choose **Telemetry > Disable Application Telemetry**.
- Wait for the sites and devices to show that telemetry has been disabled.

Step 2 Use the appliance Configuration wizard to change the cluster VIP, as follows:

- Using an SSH client, log in to the VIP address that was configured for the 10-GB interface facing the enterprise network on the Cisco DNA Center primary node. Be sure to log in on port 2222.
- When prompted, enter the Linux username and password.
- Enter the following command to access the Configuration wizard on the primary node:

```
$ sudo maglev-config update
```

If you are prompted for the Linux password, enter it again.

- Click **[Next]** until the screen prompting you for the cluster virtual IP appears. Enter the new cluster VIP, then click **[Next]** to proceed through the remaining screens of the wizard.

You must configure one virtual IP per configured interface. We recommend that you enter the `sudo maglev-config update` command so that the wizard prompts you to provide one VIP per configured interface.

When you reach the final screen, a message appears, stating that the wizard is ready to apply your changes.

- e) Click [**proceed**] to apply the cluster VIP change.

At the end of the configuration process, a success message appears and the SSH prompt reappears.

- Step 3** Restart the necessary Cisco DNA Center services by entering the following series of commands at the SSH prompt:

```
magctl service restart -d collector-netflow
magctl service restart -d collector-syslog
magctl service restart -d collector-trap
magctl service restart -d wirelesscollector
```


- Step 4** Wait for all the services to restart. You can monitor the progress of the restarts by entering the following command, substituting service names as needed for the release train appropriate for your Cisco DNA Center version.

```
magctl appstack status | grep -i -e collector-netflow -e collector-syslog -e collector-trap -e wirelesscollector
```

When all the necessary services are running, you see command output similar to the following, with a Running status for each service that has restarted successfully:


```
assurance-backend wirelesscollector-123-bc99s 1/1 Running 0 25d <IP> <IP>
ndp collector-netflow-456-lxv1x 1/1 Running 0 1d <IP> <IP>
ndp collector-syslog-789-r0rr1 1/1 Running 0 25d <IP> <IP>
ndp collector-trap-101112-3ppl1m 1/1 Running 0 25d <IP> <IP>
```

- Step 5** Access the Cisco DNA Center GUI and **Enable Application Telemetry** to all nodes as follows:

- Click the menu icon () and choose **Provision > Network Devices > Inventory**.
- Choose all the sites and devices that you want to monitor.
- From the **Actions** drop-down list, choose **Telemetry > Enable Application Telemetry**.
- Wait for the sites and devices to show that telemetry has been enabled.

Update Device Configuration Using Telemetry

You can push configuration changes to a device regardless of whether device controllability is enabled or disabled.

- Step 1** Click the menu icon () and choose **Provision > Network Devices > Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the **Global** site in the left pane, and select the site, building, or floor.

- Step 2** Choose the devices on which you want to update the configuration changes.

- Step 3** From the **Actions** drop-down list, choose **Telemetry > Update Telemetry Settings**.

The **Update Telemetry Settings** slide-in pane appears.

- Step 4** (Optional) Check the **Force Configuration Push** check box to push the configuration changes to the device.

If there is no change in the configuration settings, the existing configuration is pushed again to the device.

- Step 5** Click **Next**.

- Step 6** Choose whether to update the telemetry settings **Now** or **Later**, and then click **Apply**.

- Step 7** To preview the CLI configuration, click the **Generate Configuration Preview** radio button and do the following:
- a. In the **Task Name** field, enter a task name of your choice and click **Preview**.
You can use the created configuration preview later to deploy on selected devices.
 - b. In the **Task Submitted** dialog box, click the **View Work Items** link.
Note The dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon (≡) and choose **Activities > Work Items**.
 - c. In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
 - d. View the CLI configuration details and click **Deploy**.
 - e. Choose whether you want to deploy the device **Now** or schedule it for **Later**.
 - f. In the subsequent confirmation window, click **Yes**.

The CLI task is marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.



PART II

Discover and Manage Network Inventory and Topology

- [Discover Your Network, on page 37](#)
- [Manage Your Inventory, on page 55](#)
- [Display Your Network Topology, on page 115](#)



CHAPTER 4

Discover Your Network

- [Discovery Overview, on page 37](#)
- [Discovery Dashboard, on page 38](#)
- [Discovery Prerequisites, on page 38](#)
- [Discovery Credentials, on page 39](#)
- [Preferred Management IP Address, on page 45](#)
- [Discovery Configuration Guidelines and Limitations, on page 45](#)
- [Perform Discovery, on page 46](#)
- [Manage Discovery Jobs, on page 52](#)

Discovery Overview

The Discovery feature scans the devices in your network and sends the list of discovered devices to inventory.

The Discovery feature also works with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the devices.

There are four ways for you to discover devices:

- Use Cisco Discovery Protocol (CDP) and provide a seed IP address.
- Specify a range of IP addresses. (A maximum range of 4096 devices is supported.)
- Use Link Layer Discovery Protocol (LLDP) and provide a seed IP address.
- Use Classless Inter-Domain Routing (CIDR) and provide a seed IP address.

When configuring the Discovery criteria, remember that there are settings that you can use to help reduce the amount of time it takes to discover your network:

- **CDP Level** and **LLDP Level**: If you use CDP or LLDP as the Discovery method, you can set the CDP or LLDP level to indicate the number of hops from the seed device that you want to scan. The default, level 16, might take a long time on a large network. So, if fewer devices have to be discovered, you can set the level to a lower value.
- **Prefix Length**: If you use CIDR as a discovery method, you can set the prefix length value ranging from 20 to 30. The default value is 30.
- **Subnet Filters**: If you use an IP address range, you can specify devices in specific IP subnets for Discovery to ignore.

- **Preferred Management IP:** Whether you use CDP, LLDP, CIDR, or an IP address range, you can specify whether you want Cisco DNA Center to add any of the device's IP addresses or only the device loopback address.



Note For Cisco SD-Access Fabric and Cisco DNA Assurance, we recommend that you specify the device loopback address.

Regardless of the method you use, you must be able to reach the device from Cisco DNA Center and configure specific credentials and protocols in Cisco DNA Center to discover your devices. These credentials can be configured and saved in the **Design > Network Settings > Device Credentials** window or on a per-job basis in the **Discovery** window.



Note If a device uses a first hop resolution protocol, such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device might be discovered and added to the inventory along with its floating IP address. Later, if HSRP or VRRP fails, the IP address might be reassigned to a different device. This situation can cause issues with the data that Cisco DNA Center retrieves for analysis.

Discovery Dashboard

Click the menu icon (☰) and choose **Tools > Discovery** to view the **Discovery Dashboard**. The **Discovery Dashboard** shows the inventory overview, latest discovery, discovery type, discovery status, and recent discoveries.

Discovery Prerequisites

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by Cisco DNA Center by viewing the [Cisco DNA Center Compatibility Matrix](#).
- Understand that the preferred network latency between Cisco DNA Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)
- Ensure that at least one SNMP credential is configured on your devices for use by Cisco DNA Center. At a minimum, this can be an SNMPv2C read credential. For more information, see [Discovery Credentials, on page 39](#).
- Configure SSH credentials on the devices you want Cisco DNA Center to discover and manage. Cisco DNA Center discovers and adds a device to its inventory if at least one of the following criteria is met:
 - The account that is being used by Cisco DNA Center to SSH into your devices has privileged EXEC mode (level 15).
 - You configure the device's enable password as part of the CLI credentials configured in the Discovery job. For more information, see [Discovery Configuration Guidelines and Limitations, on page 45](#).

Discovery Credentials

Discovery credentials are the CLI, SNMPv2c, SNMPv3, HTTP(S), and NETCONF configuration values for the devices that you want to discover. You must specify the credentials based on the types of devices you are trying to discover:

- Network devices: CLI and SNMP credentials.



Note For NETCONF-enabled devices such as embedded wireless controllers, you must specify SSH credentials with admin privilege and select the NETCONF port.

- Compute devices (NFVIS): CLI, SNMP, and HTTP(S) credentials.

Because the various devices in a network can have different sets of credentials, you can configure multiple sets of credentials in Cisco DNA Center. The discovery process iterates through all sets of credentials that are configured for the Discovery job until it finds a set that works for the device.

If you use the same credential values for the majority of devices in your network, you can configure and save them to reuse in multiple Discovery jobs. To discover devices with unique credentials, you can add job-specific Discovery credentials when you run Discovery jobs. You can configure up to 10 global credentials for each credential type and define any five of them. If you need to define a job-specific credential, you can define five global credentials and one job-specific credential for each credential type.

To define credentials for a Discovery, click the menu icon (≡) and choose **Tools > Discovery > Add Discovery**. To continue, use the following procedures and discovery credential information:

- [Discover Your Network Using CDP, on page 46](#)
- [Discover Your Network Using an IP Address Range or CIDR, on page 48](#)
- [Discover Your Network Using LLDP, on page 50](#)

Table 5: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials. If authentication fails for CLI, Cisco DNA Center retries the authentication process for 300 seconds (5 minutes).
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. Note Passwords are encrypted for security reasons and are not displayed in the configuration.

Field	Description
Enable Password	<p>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</p> <p>For security reasons, re-enter the enable password.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Table 6: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Read Community: Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Write Community: Write community string used to make changes to the SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Table 7: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	<p>Security level that an SNMP message requires. Choose one of the following modes:</p> <ul style="list-style-type: none"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Auth. Type	<p>Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode.) Choose one of the following authentication types:</p> <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): Authentication based on HMAC-MD5.

Field	Description
Auth. Password	<p>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length.</p> <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	<p>Privacy type. (Enabled if you select Authentication and Privacy as Mode.) Choose one of the following privacy types:</p> <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 8: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Amount of time, in seconds, between retries.

Table 9: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .
Read	<p>You can configure up to 10 HTTPS read credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>
Write	<p>You can configure up to 10 HTTPS write credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? - <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>

Table 10: NETCONF Setting

Field	Description
Port	<p>Port on the device. You can use one of the following ports:</p> <ul style="list-style-type: none"> • Port 830 (default). • Any other port that is available on the device. • A custom port that Cisco DNA Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the Cisco DNA Center Administrator Guide.) <p>If authentication fails for NETCONF, Cisco DNA Center retries the authentication process for 300 seconds (5 minutes).</p>

Discovery Credentials and Cisco ISE

If you are using Cisco ISE as an authentication server, the Discovery feature authenticates devices using Cisco ISE as part of the discovery process. To make sure that your devices are discovered properly, follow these guidelines:

- Do not use Discovery credentials that have fewer than 4 alphanumeric characters. Although devices may have credentials with fewer than 4 alphanumeric characters, Cisco ISE allows 4 alphanumeric characters as the minimum username and password length. If the device credentials have fewer than 4 characters, Cisco DNA Center cannot collect the device's inventory data, and the device will go into a partial collection state.
- Do not use credentials that have the same username, but different passwords (cisco/cisco123 and cisco/pw123). While Cisco DNA Center allows the discovery of devices with the same username but different passwords, Cisco ISE does not allow this. If a duplicate username is used, Cisco DNA Center cannot authenticate the device and collect its inventory data, and the device will go into a partial collection state.

For information on how to define Cisco ISE as a AAA server, see [Add Cisco ISE or Other AAA Servers, on page 192](#).

Guidelines and Limitations for Discovery Credentials

The following are the guidelines and limitations for the Cisco DNA Center Discovery credentials:

- To change the device credentials used in a Discovery job, you need to edit the Discovery job and deselect the credentials that you no longer want to use. Then, you need to add the new credentials and start the discovery. For more information, see [Change Credentials in a Discovery Job, on page 52](#).
- If you change a device's credential after successfully discovering the device, subsequent polling cycles for that device fail. To correct this situation, use one of the following options:
 - Use the Discovery tool to:
 - Run a new Discovery job with job-specific credentials that match the device's new credential.
 - Edit the existing Discovery job and rerun the Discovery job.

- Use the Design tool to:
 - Create a new global credential and run a new Discovery job using the correct global credential.
 - Edit an existing global credential and use Copy & Edit to recreate the Discovery job. Alternatively, create a new Discovery job.

- If an ongoing Discovery polling cycle fails because of a device authentication failure, you can correct the situation using one of following options:
 - Use the Discovery tool to:
 - Stop or delete the current Discovery job and run a new Discovery job with job-specific credentials that match the device's credential.
 - Stop or delete the current Discovery job, edit the existing Discovery job, and rerun the Discovery job.

 - Use the Design tool to:
 - Create a new global credential and run a new Discovery job using the correct global credential.
 - Edit an existing global credential and use Copy & Edit to recreate the Discovery job. Alternately, create a new Discovery job.

- Deleting a global credential does not affect previously discovered devices. The status of the previously discovered devices does not indicate an authentication failure. However, the next Discovery job that tries to use the deleted credential will fail. The Discovery job will fail *before* it tries to contact any devices.

Discovery Credentials Example

The devices that form a typical network can have widely varying Discovery requirements. Cisco DNA Center lets you create multiple Discovery jobs to support these varying requirements. For example, assume that a network has 200 devices that form a Cisco Discovery Protocol (CDP) neighborhood. In this network, 190 devices share a global credential (Credential 0) and the remaining devices each have their own unique credential (Credential-1 through Credential-10).

For FIPS mode deployment, the discovery password must contain at least 8 characters.

To discover all the devices in this network using Cisco DNA Center, perform the following task:

-
- Step 1** Configure the CLI global credentials as Credential-0.
 - Step 2** Configure the SNMP (v2c or v3) global credentials.
 - Step 3** Run a Discovery job using one of the 190 device IP addresses (190 devices that share the global credentials) and the global Credential-0.
 - Step 4** Run 10 separate Discovery jobs for each of the remaining 10 devices using the appropriate job-specific credentials, such as Credential-1, Credential-2, Credential-3, and so on.
 - Step 5** Review the results in the **Inventory** window.
-

Preferred Management IP Address

When Cisco DNA Center discovers a device, it uses one of the device's IP addresses as the preferred management IP address. The IP address can be that of a built-in management interface of the device, another physical interface, or a logical interface such as Loopback0. You can configure Cisco DNA Center to use the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Cisco DNA Center.

When you choose **Use Loopback IP** as the preferred management IP address, Cisco DNA Center determines the preferred management IP address as follows:

- If the device has one loopback interface, Cisco DNA Center uses that loopback interface IP address.
- If the device has multiple loopback interfaces, Cisco DNA Center uses the loopback interface with the highest IP address.
- If there are no loopback interfaces, Cisco DNA Center uses the Ethernet interface with the highest IP address. (Subinterface IP addresses are not considered.)
- If there are no Ethernet interfaces, Cisco DNA Center uses the serial interface with the highest IP address.

After a device is discovered, you can update the management IP address from the **Inventory** window. For more information, see [Update a Device's Management IP Address, on page 100](#).

Discovery Configuration Guidelines and Limitations

The following are the guidelines and limitations for Cisco DNA Center to discover your Cisco Catalyst 3000 Series Switches and Catalyst 6000 Series Switches:

- Configure the CLI username and password with privileged EXEC mode (level 15). These credentials are the same CLI username and password that you configure in Cisco DNA Center for the Discovery function. Cisco DNA Center requires the highest access level to the device.
- Explicitly specify the transport protocols allowed on individual interfaces for both incoming and outgoing connections. Use the **transport input** and **transport output** commands for this configuration. For information about these commands, see the command reference document for the specific device type.
- Do not change the default login method for a device's console port and the VTY lines. If a device is already configured with a AAA (TACACS) login, make sure that the CLI credential defined in the Cisco DNA Center is the same as the TACACS credential defined in the TACACS server.

The following are the guidelines and limitations for Cisco DNA Center to discover your wireless controllers and APs:

- Cisco Wireless Controllers must be discovered using the management IP address instead of the service port IP address. If not, the related wireless controller 360 and AP 360 windows will not display any data.
- After the wireless controllers are discovered, Cisco DNA Center displays the list of associated APs in the inventory. The listed APs are connected to the wireless controller during either the discovery or through inventory sync. To view any new APs that join the wireless controller after the inventory sync, you must perform a manual resync.



Note This limitation is applicable only for the devices that are not yet assigned to a site or provisioned in Cisco DNA Center.

Perform Discovery

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, or an IP address range.

Your devices must have the required device configurations, as described in [Discovery Prerequisites, on page 38](#).

- For IP address range discovery, only ping-reachable devices are included in the list of discovered devices. Ping-unreachable devices are ignored and aren't included in the list of discovered devices.
- For CDP- and LLDP-based discovery, because CDP and LLDP protocols respond to even ping-unreachable IPs, ping-unreachable devices are included in the list of discovered devices.
- For CDP- and LLDP-based discovery, configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)
- The Discovery function requires the correct SNMP read-only community string. If an SNMP read-only community string is not provided, as a *best effort*, the Discovery function uses the default SNMP read-only community string, public.
- During discovery, devices that are already discovered and associated with a site are skipped for site assignment.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.
- During discovery using SNMPv3 credentials, Cisco DNA Center pushes the SNMPv3 credentials with the default SNMP user group to the device ignoring the existing user group on the device.

Discover Your Network Using CDP


You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, or LLDP. This procedure shows you how to discover devices and hosts using CDP. For more information about the other discovery methods, see [Discover Your Network Using an IP Address Range or CIDR, on page 48](#) and [Discover Your Network Using LLDP, on page 50](#).



-
- Note**
- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
 - CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.
-

Before you begin

- Enable CDP on your network devices.
- Configure your network devices, as described in [Discovery Prerequisites, on page 38](#).
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1 Click the menu icon () and choose **Tools > Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **Let's Get Ready** window, click **Next**.

Step 4 In the **Discover Devices** window, complete the following fields:

- Enter a name for the discovery job.
- Under **Discovery Type**, choose **CDP**.
- In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.
- (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

You can enter addresses either as an individual IP address ($x.x.x.x$) or as a classless inter-domain routing (CIDR) address ($x.x.x.x/y$), where $x.x.x.x$ refers to the IP address and y refers to the subnet mask. The subnet mask can be a value from 0 to 32.

- Click .

Repeat Step d and Step e to exclude multiple subnets from the Discovery job.

- (Optional) In the **CDP Level** field, enter the number of hops from the seed device that you want to scan.

Valid values are from 1 to 16. The default value is 16. For example, CDP level 3 means that CDP will scan up to three hops from the seed device.

- For **Preferred Management IP**, choose one of the following options:

- **None**: Allows the device to use any of its IP addresses.
- **Use Loopback IP**: Specify the device's loopback interface IP address.

Note If you choose **Use Loopback IP** and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in [Preferred Management IP Address, on page 45](#).

Note To use the loopback interface IP address as the preferred management IP address, make sure that the CDP neighbor's IP address is reachable from Cisco DNA Center.

Step 5 In the **Provide Credentials** window, enter at least one CLI credential and one SNMP credential that Cisco DNA Center will configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see [Discovery Credentials, on page 39](#).

Step 6 In the **Advanced Settings** window, do the following:

- Protocol Order**: Choose **SSH** or **Telnet**. If you choose both, you can specify the order in which they are used by dragging the protocols up or down.

- b) Configure the **SNMP Polling Properties**. Use the global SNMP polling properties defined in the **Network Settings > Device Credentials** window or modify for this discovery instance.

Step 7 In the **Assign Devices to Site** window, do any one of the following:

- **Assign devices to an existing site:** Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area.
- **Assign devices to a new site:** Click the **Already have an area** radio button or **Create a new area** radio button and complete the required fields.
- **Skip site assignment for now:** Use this option if you want the devices to be assigned to sites later from inventory.

Step 8 In the **Schedule Job** window, do the following:

- a) Click the toggle button to enable or disable **Discover new devices only** option.
- b) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you choose the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Start Discovery**.


You can view the status of the task in the **Activities** window.

Discover Your Network Using an IP Address Range or CIDR

You can discover devices using an IP address range, CIDR, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range or CIDR. For more information about the other Discovery methods, see [Discover Your Network Using CDP, on page 46](#) and [Discover Your Network Using LLDP, on page 50](#).

Before you begin


Your devices must have the required device configurations, as described in [Discovery Prerequisites, on page 38](#).

Step 1 Click the menu icon () and choose **Tools > Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.


Step 3 In the **Let's Get Ready** window, click **Next**.

Step 4 In the **Discover Devices** window, complete the following fields:

- a) Enter a name for the discovery job.
- b) Under **Discovery Type**, choose **IP Address/Range**.
- c) If you choose **IP Address/Range** discovery type, do the following:
1. In the **From** and **To** fields, enter the beginning and ending IP addresses (IP address range) for Cisco DNA Center to scan, and click .

You can enter a single IP address range or multiple IP addresses for the discovery scan.

Note Cisco Wireless Controllers must be discovered using the Management IP address instead of the Service Port IP address. If not, the related wireless controller 360 and AP 360 pages will not display any data.

2. (Optional) Repeat the previous step to enter additional IP address ranges.
- d) If you choose **CIDR** discovery type, do the following:
1. In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.
 2. (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.
You can enter addresses either as an individual IP address ($x.x.x.x$) or as a classless inter-domain routing (CIDR) address ($x.x.x.x/y$), where $x.x.x.x$ refers to the IP address and y refers to the subnet mask. The subnet mask can be a value from 0 to 32.
 3. Click .
Repeat the previous step to exclude multiple subnets from the Discovery job.
 4. In the **Prefix Length** field, enter the value of prefix length. The valid value ranges from 20 to 30.
- e) For **Preferred Management IP Address**, choose one of the following options:
- **None**: Allows the device to use any of its IP addresses.
 - **Use Loopback IP**: Specify the device's loopback interface IP address.
- Note** If you choose **Use Loopback IP** and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in [Preferred Management IP Address, on page 45](#).

Step 5 In the **Provide Credentials** window, enter at least one CLI credential and one SNMP credential that Cisco DNA Center will configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see [Discovery Credentials, on page 39](#).

Step 6 In the **Advanced Settings** window, do the following:

- a) **Protocol Order**: Choose **SSH** or **Telnet**. If you choose both, you can specify the order in which they are used by dragging the protocols up or down.
- b) Configure the **SNMP Polling Properties**. Use the global SNMP polling properties defined in the **Network Settings > Device Credentials** window or modify for this discovery instance.

Step 7 In the **Assign Devices to Site** window, do any one of the following:

- **Assign devices to an existing site**: Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area.
- **Assign devices to a new site**: Click the **Already have an area** radio button or **Create a new area** radio button and complete the required fields.
- **Skip site assignment for now**: Use this option if you want the devices to be assigned to sites later from inventory.

Step 8 In the **Schedule Job** window, do the following:

- a) Click the toggle button to enable or disable **Discover new devices only** option.
- b) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you choose the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Start Discovery**.

You can view the status of the task in the **Activities** window.

Discover Your Network Using LLDP

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, or an IP address range. This procedure shows you how to discover devices and hosts using LLDP. For more information about the other discovery methods, see [Discover Your Network Using CDP, on page 46](#) and [Discover Your Network Using an IP Address Range or CIDR, on page 48](#).



Note

- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.
- CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable LLDP on your network devices.
- Configure your network devices, as described in [Discovery Prerequisites, on page 38](#).
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1 Click the menu icon (☰) and choose **Tools > Discovery**.

Step 2 In the **Discovery** window, click **Add Discovery**.

Step 3 In the **Let's Get Ready** window, click **Next**.

Step 4 In the **Discover Devices** window, complete the following fields:

- Enter a name for the discovery job.
- Under **Discovery Type**, choose **LLDP**.
- In the **IP Address** field, enter a seed IP address for Cisco DNA Center to start the Discovery scan.
- (Optional) In the **Subnet Filter** field, enter an IP address or subnet to exclude from the Discovery scan.

You can enter addresses either as an individual IP address ($x.x.x.x$) or as a classless inter-domain routing (CIDR) address ($x.x.x.x/y$), where $x.x.x.x$ refers to the IP address and y refers to the subnet mask. The subnet mask can be a value from 0 to 32.

- Click .

Repeat Step c and Step d to exclude multiple subnets from the Discovery job.

- f) (Optional) In the **LLDP Level** field, enter the number of hops from the seed device that you want to scan.

Valid values are from 1 to 16. The default value is 16. For example, LLDP level 3 means that LLDP will scan up to three hops from the seed device.

- g) For **Preferred Management IP**, choose one of the following options:

- **None**: Allows the device use any of its IP addresses.
- **Use Loopback IP**: Specify the device's loopback interface IP address.

Note If you choose this option and the device does not have a loopback interface, Cisco DNA Center chooses a management IP address using the logic described in [Preferred Management IP Address, on page 45](#).

Note To use the loopback interface IP address as the preferred management IP address, make sure that the LLDP neighbor's IP address is reachable from Cisco DNA Center.

Step 5 In the **Provide Credentials** window, enter at least one CLI credential and one SNMP credential that Cisco DNA Center will configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see [Discovery Credentials, on page 39](#).

Step 6 In the **Advanced Settings** window, do the following:

- a) **Protocol Order**: Choose **SSH** or **Telnet**. If you choose both, you can specify the order in which they are used by dragging the protocols up or down.
- b) Configure the **SNMP Polling Properties**. Use the global SNMP polling properties defined in the **Network Settings > Device Credentials** window or modify for this discovery instance.

Step 7 In the **Assign Devices to Site** window, do any one of the following:

- **Assign devices to an existing site**: Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area.
- **Assign devices to a new site**: Click the **Already have an area** radio button or **Create a new area** radio button and complete the required fields.
- **Skip site assignment for now**: Use this option if you want the devices to be assigned to sites later from inventory.

Step 8 In the **Schedule Job** window, do the following:

- a) Click the toggle button to enable or disable **Discover new devices only** option.
- b) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.

If you choose the **Daily** or **Weekly** recurrence option, the **Discover new devices only** option is disabled.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Start Discovery**.

You can view the status of the task in the **Activities** window.

Manage Discovery Jobs

The following sections provide information about how to manage the Discovery jobs.

Stop and Start a Discovery Job

-
- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
 - Step 2** To stop an active Discovery job, hover your cursor over the ellipsis icon (⋮) in the **Actions** column and choose **Stop Discovery**.
 - Step 3** To restart an inactive Discovery job, hover your cursor over the ellipsis icon (⋮) in the **Actions** column and choose **Re-discover**.
-

Change Credentials in a Discovery Job

You can change the credentials used in a Discovery job and then rerun the Discovery job.

Before you begin

You should have created at least one Discovery job.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
 - Step 2** To copy a Discovery job, hover your cursor over the ellipsis icon (⋮) in the **Actions** column and choose **Copy & Edit**.
Cisco DNA Center creates a copy of the Discovery job, named Clone of *Discovery_Job*.
 - Step 3** (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.
 - Step 4** In the **New Discovery** window, expand the **Credentials** area and choose any of the global credentials that have already been created, or configure your own.
If you want to use existing credentials, make sure that to select them. If you don't want to use a credential, deselect it.
 - Step 5** To configure your own credentials, click **Add Credentials**.
You must configure CLI and SNMPv2c credentials. All other credentials are optional. For field information, see [Discovery Credentials, on page 39](#).
To save credentials for *only* the current job, click **Save**. To save them for the current job and future jobs, check the **Save as global settings** check box and then click **Save**.
 - Step 6** Click **Discover**.
-

Clone a Discovery Job

You can clone a Discovery job and retain all the information defined for that job.

Before you begin

Run at least one Discovery job.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
- Step 2** To copy a Discovery job, hover your cursor over the ellipsis icon (⋮) in the **Actions** column and choose **Copy & Edit**.
Cisco DNA Center creates a copy of the Discovery job, named Clone of *Discovery_Job*.
- Step 3** (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.
- Step 4** Define or update the parameters for the new Discovery job.
-

Delete a Discovery Job

You can delete a Discovery job whether it is active or inactive.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Discovery**.
- Step 2** To delete a Discovery job, hover your cursor over the ellipsis icon (⋮) in the **Actions** column and choose **Delete**.
- Step 3** Click **OK** to confirm.
-



CHAPTER 5

Manage Your Inventory

- [About Inventory, on page 56](#)
- [Inventory and Cisco ISE Authentication, on page 56](#)
- [Display Information About Your Inventory, on page 57](#)
- [Manage User-Defined Fields, on page 71](#)
- [Launch Topology Map from Inventory, on page 72](#)
- [Types of Devices in the Cisco DNA Center Inventory, on page 72](#)
- [Filter Devices, on page 89](#)
- [Manage Devices in Inventory, on page 90](#)
- [Configure a REP Ring for Devices, on page 93](#)
- [Create Port Groups, on page 94](#)
- [Assign Tags to Ports, on page 95](#)
- [Port Usage Information, on page 95](#)
- [Maintenance Mode for Devices, on page 96](#)
- [Inventory Insights, on page 97](#)
- [Manage System Beacon, on page 99](#)
- [Change the Device Role \(Inventory\), on page 99](#)
- [Update a Device's Management IP Address, on page 100](#)
- [Update the Device Polling Interval, on page 101](#)
- [Resynchronize Device Information, on page 102](#)
- [Delete a Network Device, on page 102](#)
- [Launch Command Runner \(Inventory\), on page 103](#)
- [Troubleshoot Device Reachability Issues Using Run Commands, on page 103](#)
- [Use a CSV File to Import and Export Device Configurations, on page 104](#)
- [Configuration Drift of a Device, on page 106](#)
- [View Configuration Drift of a Device, on page 107](#)
- [Label Configuration Drift, on page 108](#)
- [Replace a Faulty Device, on page 109](#)
- [Replace a Faulty Access Point, on page 111](#)
- [Limitations of the RMA Workflow in Cisco DNA Center, on page 112](#)
- [Reboot Access Point, on page 113](#)

About Inventory

The Inventory function retrieves and saves details, such as host IP addresses, MAC addresses, and network attachment points about devices in its database.

The Inventory feature can also work with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the device.

Inventory uses the following protocols, as required:

- Link Layer Discovery Protocol (LLDP).
- IP Device Tracking (IPDT) or Switch Integrated Security Features (SISF). (IPDT or SISF must be enabled on the device.)
- LLDP Media Endpoint Discovery. (This protocol is used to discover IP phones and some servers.)
- Network Configuration Protocol (NETCONF). For a list of devices, see [Discovery Prerequisites, on page 38](#).

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default interval is every 24 hours. However, you can change this interval as required for your network environment. For more information, see [Update the Device Polling Interval, on page 101](#). Also, a configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than one day are displayed. This prevents stale device data, if any, from being displayed. On average, polling 500 devices takes approximately 20 minutes.

Inventory and Cisco ISE Authentication

Cisco ISE has two different use cases in Cisco DNA Center:

- If your network uses Cisco ISE for device authentication, you need to configure the Cisco ISE settings in Cisco DNA Center. As a result, when provisioning devices, Cisco DNA Center configures the devices with the Cisco ISE server information that you defined. In addition, Cisco DNA Center configures the devices on the Cisco ISE server and propagates subsequent updates to the devices. For information about configuring Cisco ISE settings in Cisco DNA Center, see [Configure Global Network Servers, on page 193](#).



Note If you are using Cisco ISE for authenticating Cisco Catalyst 9800 series devices, you must configure Cisco ISE to provide privilege for NETCONF users.

If a device is not configured or updated on the Cisco ISE server as expected due to a network failure or the Cisco ISE server being down, Cisco DNA Center automatically retries the operation after a certain wait period. However, Cisco DNA Center does not retry the operation if the failure is due to a rejection from Cisco ISE, as an input validation error.

When Cisco DNA Center configures and updates devices in the Cisco ISE server, the transactions are captured in the Cisco DNA Center audit logs. You can use the audit logs to help troubleshoot issues related to the Cisco DNA Center and Cisco ISE inventories.

After you provision a device, Cisco DNA Center authenticates the device with Cisco ISE. If Cisco ISE is not reachable (no RADIUS response), the device uses the local login credentials. If Cisco ISE is reachable, but the device does not exist in Cisco ISE or its credentials do not match the credentials configured in Cisco DNA Center, the device does not fall back to use the local login credentials. Instead, it goes into a partial collection state.

To avoid this situation, make sure that before you provision devices using Cisco DNA Center, you have configured the devices in Cisco ISE with the same device credentials that you are using in Cisco DNA Center. Also, make sure that you configured valid discovery credentials. For more information, see [Discovery Credentials, on page 39](#).

- If required, you can use Cisco ISE to enforce access control to groups of devices.

Display Information About Your Inventory





You can display and filter for information about discovered devices in your inventory. You can also customize or change the information displayed in the **Devices** table.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 (Optional) To change the Inventory view, use the toggle button (☰    ) in the top-right corner. You can change your default view (the list layout) to other layouts, such as the topology or map layout.

Step 3 (Optional) To change the **Devices** table's focus views, from the **Focus** drop-down list, choose a view, such as **Default**, **Inventory**, or **Software Images**.

Note

- The displayed columns change depending on the chosen focus view.
- Selected devices persist in each new focus view.

Step 4 (Optional) To filter for specific device details in the **Devices** table, you can do the following:

- To filter for a device family, choose one or more of the device family buttons at the top of the **Inventory** window. For example, you can click **Routers** to display only routers in the table.
- To filter for device work items, in the left pane, check the check box of one or more work items. The table is immediately filtered for the work item. For example, you can check the **Unreachable** check box to display only unreachable devices in the table.
- To filter for specific device details, click **Filter devices** and choose from the filter options: **Quick Filters**, **Advanced Filters**, or **Recent Filters**. Then click **Apply**.

For more information, see [Filter Devices, on page 89](#).

Step 5 (Optional) To take a guided tour of the **Inventory** window, click **Take a tour** in the top-right corner.

Step 6 (Optional) To export all the data in the **Devices** table, click **Export** in the top-right corner.


Step 7 (Optional) To customize the **Devices** table, click the settings icon (⚙️) in the top-right corner, choose from the following options in the **Table Settings** slide-in pane, and then click **Apply**.

- **Table Appearance:** Choose if you want the default or compact table view and table striping.
- **Edit Table Columns:** Choose if you want to create a custom view and if you want to hide or display columns. Note that the column selection does not persist across sessions.

The following table provides key information relevant to certain table columns.

Column	Description
Device Name	<p>Name of the device.</p> <p>Click the device name for more information about that device.</p> <p>Note A device name that is displayed in red means that inventory has not polled the device and updated its information for more than 30 minutes.</p>
Support Type	<p>Shows the device support level:</p> <ul style="list-style-type: none"> • Supported: The device pack is tested for all applications on Cisco DNA Center. You can open a service request if any of the Cisco DNA Center functionalities for these devices do not work. • Limited: The device pack for legacy devices is tested only for the following features and tested only on a best-effort basis on Cisco DNA Center. <ul style="list-style-type: none"> • Discovery • Topology • Device Reachability • Config Change Audit • Inventory • Software Image Management (Software images may not be available for EOL devices on cisco.com. Not recommended for EOL devices.) • Template Provisioning (Applicable only for switches.) <p>For more information, see the Cisco DNA Center Legacy Device Compatibility Matrix.</p> <ul style="list-style-type: none"> • Unsupported: All remaining Cisco and third-party devices that are not tested and certified on Cisco DNA Center. You can try out various functionalities on Cisco DNA Center for these devices, as a best effort. However, you cannot raise a service request or a bug if Cisco DNA Center features do not work as expected. • Third Party: Device pack is built by customers or business partners and goes through the certification process. Third-party devices support base automation capabilities such as Discovery, Inventory, Topology, and so on. Cisco TAC provides an initial level of support for these devices. However, if there is a problem with the device pack, you need to contact the business partner. <p>For more information, see the Cisco DNA Center Compatibility Matrix.</p>

Column	Description
Reachability	<p>The following is a list of the various statuses:</p> <ul style="list-style-type: none"> • Reachable: The device is reachable by Cisco DNA Center using SNMP, HTTP(S), and NETCONF polling. • Ping Reachable: The device is reachable by Cisco DNA Center using ICMP polling and not reachable using SNMP, HTTP(S), and NETCONF polling. • Unreachable: The device is not reachable using SNMP, HTTP(S), NETCONF, or ICMP polling.
EoX Status	<p>Shows the EoX scan status:</p> <ul style="list-style-type: none"> • Success: The device is scanned for EoX alerts successfully. • Not Scanned: The device is not scanned for EoX alerts. • Scan Failed: Cisco DNA Center is not able to scan the device for EoX alerts. • Scanning: Cisco DNA Center is scanning the device for EoX alerts. <p>Hover your cursor over the i icon next to EoX Status, and click Click here to accept to initiate an EoX scan.</p> <p>For the devices that are scanned successfully, the EoX Status column shows the number of alerts, if any. Click the number of alerts to view the alerts in detail.</p> <p>In the slide-in pane, click the Hardware, Software, and Module tabs to view the hardware, software, and module EoX alerts.</p>
Manageability	<p>Shows the device status:</p> <ul style="list-style-type: none"> • Managed with green tick icon: Device is reachable and is fully managed. • Managed with orange error icon: Device is managed with some error, such as unreachable, authentication failure, missing NETCONF ports, internal error, and so on. Hover your cursor over the error message to view more details about the error and the impacted applications. • Unmanaged: Device cannot be reached and no inventory information was collected because of device connectivity issues.
Platform	Cisco product part number.
Device Role	<p>Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Cisco DNA Center is unable to determine a device role, it sets the device role to Unknown.</p> <p>Note If you manually change the device role, the assignment remains static. Cisco DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization.</p> <p>If required, you can use the drop-down list in this column to change the assigned device role.</p>
Site	<p>The site to which the device is assigned. Click Assign if the device is not assigned to any site. Click Choose a Site, select a site from the hierarchy, and click Save. For more information, see Network Hierarchy Overview, on page 125.</p>

Column	Description
Last Updated	Most recent date and time on which Cisco DNA Center scanned the device and updated the database with new information about the device.
Resync Interval	The polling interval for the device. Set the resync interval from the Inventory window by choosing Actions > Edit Device > Resync Interval . To set the resync type as Global , from the main menu, choose System > Settings . For more information, see the Cisco DNA Center Administrator Guide .
Provisioning Status	<p>Shows the status of the last provisioning operation attempted on a device. Click See Details to view the status of past provisioning operations.</p> <ul style="list-style-type: none"> • Success: The latest operation on the device was successful. • Success with a warning icon: The latest operation on the device was successful, but there are failures from past provisioning operations that may need user attention. • Failed: The latest operation on the device has failed. • Failed with a warning icon: The latest operation on the device has failed, and there are failures from past provisioning operations that may need user attention. • Configuring: The device is currently being configured. • Pending: The system is trying to determine if the device will be impacted by an ongoing provisioning operation. • Not Provisioned: The device has never been provisioned. • Out of Sync: The network settings or network profiles for a device have been modified after the last provisioning operation.
Credential Status	<p>Shows the device credential status:</p> <ul style="list-style-type: none"> • Not Applied: The device credential is not applied on the device. • Success: The device credential is applied on the device successfully. • Failed: The device credential failed on the device. <p>Click See Details to view the details about the credentials.</p> <p>The Credential Status slide-in pane shows the Type, Name/Description, Status, and Details of the credential.</p> <p>For a device whose status is Failed, hover your cursor over the ellipsis icon () in the Actions column and choose Retry or Clear.</p> <ul style="list-style-type: none"> • Retry: Applies the credential on the device. • Clear: Clears the device credential.
AP CDP Neighbors	Displays details about the switch and port connected to an AP in the Inventory window. This window displays information about AP CDP neighbors even if the connected access switch is managed by Cisco DNA Center.

- **Edit Custom Views:** First you must create a custom view in the **Edit Table Columns** tab, and then you can edit the custom view.
- **Reset All Settings:** Reset the table settings to the default settings.

Step 8 (Optional) To manage your devices from the **Devices** table, you can use the following options:

Name	Description
Add Device	<p>You can click Add Device to add a network or compute device, or integrate a Meraki dashboard or Firepower Management Center (FMC) with Cisco DNA Center.</p> <p>For more information, see Types of Devices in the Cisco DNA Center Inventory, on page 72.</p>
Tag	<p>You can click Tag to tag devices, edit and delete tags, or create port groups.</p> <p>For more information, see Manage Devices in Inventory, on page 90.</p>
Actions drop-down list	<p>You can use the Actions drop-down list to manage your devices, software images, telemetry, and more.</p> <p>To view more details about each action option, click the right-adjacent information icon (ⓘ).</p>

Step 9 (Optional) In the **Devices** table, you can do the following:

- To sort the columns in either ascending or descending order, click the column header.
- To view more details about a device, click the device name and then click **View Device Details**.
- To view a device's compliance details, click either **Non-Compliant** or **Compliant** under the **Compliance** column.
- To assign a site to a device, click **Assign** under the **Site** column.
- To change a device role, click the edit icon under the **Device Role** column and then choose from the options, such as **ACCESS** or **CORE**.
- To mark an image as Golden or view its needed updates, click **Mark Golden** or **Needs Update** under the **Software Image** column.
- To change the number of entries, scroll down to the bottom of the window, and from the **Show Records** drop-down list, choose the number of entries that you want displayed.

Note that if there are more than 25 entries in the table and you choose a different focus view, the same number of entries is displayed in each new view.

Note Each focus view displays different columns, and you can customize a table view to include columns, such as **Compliance**, **Site**, **Device Role**, and **Software Image**.

Display Information About a Device

You can display, filter, and search for information about a discovered device, its security, and its compliance.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon () and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.



Step 2 In the **Devices** table, click the name of a device and more information about the device is displayed.



Step 3 Click **View Device Details**.

The device details are displayed in the window.

Step 4 Use the following table that describes the available information in this window to display, filter, and search for details about a device.

Name	Description
Run Commands	<p>This link is only available for routers, wireless controllers, switches, and hubs.</p> <p>Launch the Command Runner application to run diagnostic CLI commands and view the resulting command output on a device.</p> <p>To launch Command Runner, you must have installed the Command Runner application. For more information, see the Cisco DNA Center Administrator Guide.</p>
Learn WLC Config	<p>This link is only available for wireless controllers.</p> <p>Click the link to open Learn Device Configuration window, where you can provision a wireless controller.</p> <p>To open this window, the wireless controller must be reachable and in a Managed state.</p>
View 360	<p>This link is available for all devices.</p> <p>Displays the Device 360 window for that device.</p> <p>To open this window, you must have installed the Assurance application.</p>
Interfaces	<p>This tab is available for all devices except APs.</p> <p>Displays information about the device's ports, such as its Ethernet ports, in a topology or table view.</p> <p>For more information about device interfaces, see Display Information About a Device's Interface, on page 66.</p>

Name	Description
Hardware & Software	<p>This tab is available on all devices.</p> <p>Displays the device's hardware and software details, such as its uptime and provision status, with an operational summary.</p>
Configuration	<p>This tab is only available for APs, routers, switches, and hubs.</p> <p>For routers, switches, and hubs, this tab displays detailed configuration information that is similar to what is displayed in the output of the show running-config command. You can hide line numbers, search for a command line or piece of text, or export the CLI output.</p> <p>For APs, this tab displays information about the AP configuration, 2.4-GHz radio configuration, and 5-GHz radio configuration.</p> <p>This feature is not supported for wireless controllers, so configuration data is not returned for this device type.</p>
Power	<p>This tab is only available for routers, switches, and hubs.</p> <p>Displays details about the device's power usage and supplies.</p> <p>To specify or narrow down the data in the Power Supplies table, you can either:</p> <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display power supplies by any combination of values, such as values for the Name, Operational Status, and Serial Number fields.
Fans	<p>This tab is only available for routers, switches, and hubs.</p> <p>Displays details about fans.</p> <p>To specify or narrow down the data in the Fans table, you can either:</p> <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display fans by any combination of values for the Name and Operational Status fields.

Name	Description
SFP Modules	<p>This tab is only available for routers, switches, and hubs.</p> <p>Displays details such as the manufacturer and the ports that Small Form-Factor Pluggable (SFP) modules are connected to.</p> <p>To specify or narrow down the data in the SFP Modules table, you can either:</p> <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display SPF modules by any combination of values, such as values for the Name, Platform, and Serial Number fields.
User Defined Fields	<p>This tab is available for all devices.</p> <p>Displays the user-defined fields that are associated with the device.</p> <p>Click Manage User Defined Fields to display the Manage User Defined Fields slide-in pane. You can do the following:</p> <ul style="list-style-type: none"> • Click Create New Fields to create a new field. • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display user-defined fields by any combination of values, such as values for the Name, Description, and Action fields. <p>To add a user-defined field to a device, you first must create a user-defined field in the Manage User Defined Fields slide-in pane. For more information, see Create User-Defined Fields, on page 71.</p> <p>To display a user-defined field, you must assign it to a device and add a value to it. For more information, see Add User-Defined Fields to a Device, on page 72.</p>
Config Drift	<p>This tab is available for all devices.</p> <p>Displays configuration changes on the device, including a change history, and compares two configuration versions. You can do the following:</p> <ul style="list-style-type: none"> • Label the configuration drift on the time line for future reference. For more information, see Label Configuration Drift, on page 108. • Pick any two versions of the same device and compare their running configuration data.

Name	Description
REP Rings	<p>This tab is available for all devices.</p> <p>Displays details about Resilient Ethernet Protocol (REP) rings, such as its name, ring size, first adjacent device, and so on.</p> <p>Click Create REP Ring and follow the workflow to create a REP ring.</p> <p>For more information, see Delete a Node from a REP Ring, on page 502 or Delete a REP Ring, on page 502.</p>
Wireless Info	<p>This tab is only available for wireless controllers.</p> <p>Displays details about managed sites, wireless, redundancy, health parameters, and more.</p> <p>In the Wireless Summary tab, in the SSIDs table, you can search for a specific value by clicking Search Table, manually entering a value, and then pressing the Enter key. The narrowed search results are displayed with the value highlighted throughout the table.</p>
Mobility	<p>This tab is only available for wireless controllers.</p> <p>Displays mobility details, such as the mobility group name, RF group name, and so on.</p> <p>The Mobility Peers table is displayed if mobility peers are configured on the device. If mobility peers are not configured, see Configure Mobility Group, on page 418.</p> <p>You can filter the table to display specific mobility peers by any combination of values, such as values for MAC address, Device Name, and IP Address fields.</p>
Advisories	<p>This tab is available for all devices.</p> <p>Displays a device's advisory details in the Advisories table. You can do the following:</p> <ul style="list-style-type: none"> • Click Manage All to display the Security Advisories window to manage your devices and advisories. • Click Filter to display advisories by any combination of values, such as values for the Advisory ID and Advisory Title fields. Then click Apply. • Click an advisory ID to display more information about that advisory. • In the Custom Match Pattern column, click Add match pattern to add or update a condition to match with devices in the CONDITIONS text box. Then you can save the match pattern and run a scan to check the number of devices that match with the match pattern.

Name	Description
Summary	<p>This tab is available for all devices.</p> <p>Displays a device's compliance summary, such as when compliance last ran for the Startup vs Running configuration. You can do the following:</p> <ul style="list-style-type: none"> • Click Run Compliance Check to check the device for compliance. • Click View Preference for Acknowledged Violations to view the list of acknowledged violation attributes. You can unlist a violation to open it.

Display Information About a Device's Interface

For routers, wireless controllers, switches, or hubs, you can display, search, and filter for information about a device's interface. Depending on the device, certain information is available.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.



The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 In the **Devices** table, click the name of a device, and then click **View Device Details**.

Step 3 In the left pane, expand **Interfaces**.


Step 4 Use the following table that describes the **Interfaces** drop-down list options to display details about an interface.


Name	Description
Ethernet Ports	<ul style="list-style-type: none"> • This tab is available for all devices except APs. • Displays Ethernet ports details in two views: topology and table. <ul style="list-style-type: none"> • The topology view displays the Ethernet port topology of a device with a color-coded system of each port's connection status. • The table view displays Ethernet ports details, such as the ports' operational status, admin status, and so on. • For more information about the two views, see Display Information About Ethernet Ports, on page 67.

Name	Description
VLANs	<ul style="list-style-type: none"> • This tab is only available for switches and hubs. • Displays VLAN details, such as its operational status and admin status, in table format. • The VLANs table displays the ID of the following types of VLANs: <ul style="list-style-type: none"> • VLAN ID of the manufacturing-supplied default VLAN • VLAN ID of the configured default VLAN • VLAN ID of the configured VLAN <p>To specify or narrow down the data in the VLANs table, you can either:</p> <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display VLANs by any combination of values, such as values for the VLAN Name, VLAN ID, and Operational Status fields.
Virtual Ports	<ul style="list-style-type: none"> • This tab is only available for wireless controllers and routers. • Displays details about ports, such as its operational status, admin status, and so on. • To specify or narrow down the data in the VLANs table, you can either: <ul style="list-style-type: none"> • Click Search Table, manually enter a value, and then press the Enter key. The narrowed search results are displayed with the value highlighted throughout the table. • Click the filter icon () to display virtual ports by any combination of values, such as values for the Port Name, Operational Status, and Admin Status fields.

Display Information About Ethernet Ports

In the **Ethernet Ports** tab, you can display, search, and filter for certain information about a port or ports through either the topology view or table view.

- Step 1** Click the menu icon () and choose **Provision > Inventory**.
- Step 2** In the **Devices** table, click a device name, and then click **View Device Details**.
- Step 3** In the left pane, expand **Interfaces** and choose **Ethernet Ports**.

Step 4 In the upper-right corner, click **Topology View** () to view the Ethernet port topology if it's not already displayed. This view displays the Ethernet port topology of a device with a color-coded system of each port's connection status. Hover your cursor over a port for more details.

Note For Cisco Catalyst 4000 Series, 6000 Series, and 9000 Series Switches and Cisco ASR 1000 Series Aggregation Services Routers, this view displays line cards and supervisor cards details, such as the part number and serial number, if the cards are available.

Step 5 In the topology view, you can do the following:

- To view the error reason for an error-disabled port, click the port.
- To filter for a specific Ethernet port, use the **Color Code** drop-down list. The following table describes the available drop-down list options.


Table 11: Color Code Drop-Down List Options

Name	Description
Status	Displays the default view of the topology view.
Access VLANs	Displays the access VLAN assigned to a particular port. The Access VLANs view allows you to select a maximum of five access VLANs and lists only the access VLANs associated with the port. This option displays the access VLANs in the following color-coded system: Selected , Not Configured , Default , and VLAN .
Port Channels	Displays the top five port channels that are configured on the device. This option only displays the configured port channels on the device in the following color-coded system: Selected and Port-channel with a corresponding number.

Step 6 In the upper-right corner, click **Table View** () to view the **Ports** table.

The **Ports** table displays Ethernet ports details, such as a ports' operational status, admin status, and so on.

Step 7 (Optional) To specify or narrow down the data in the **Ports** table, you can:

- Click **Search Table**, manually enter a value, and then press the **Enter** key. The narrowed search results are displayed with the value highlighted throughout the table.
- Click the filter icon () to display ports by any combination of values, such as values for the **Tags**, **Port Name**, and **Type** fields. Enter the wanted values, and click **Search**.

Step 8 (Optional) In the table view, you can do the following:

- Click **Tag** to tag a port or ports, search for a tag, or manage tags.

For more information, see [Assign Tags to Ports, on page 95](#).

- Click **Export** to export the **Ports** table data.

Manage Port Details

You can manage and edit certain port details of a device.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

Step 2 In the **Devices** table, click a device name, and then click **View Device Details**.

Step 3 In the left pane, expand **Interfaces** and choose **Ethernet Ports**.

Step 4 Click a port in the topology view (🏠 📄), or click a port name in the table view (🏠 📄).

Information about the port is displayed.

- Note**
- For Cisco Catalyst 2000, 3000, and 9000 Series Switches, port details include the port's maximum allocated power and power drawn.
 - This window displays the details of the CDP neighbor. If CDP is not present, the LLDP neighbor details displays. If both CDP and LLDP neighbors are not present, the **Neighbor Details** area is hidden from this window.

Step 5 (Optional) Click **Tag** to tag the port, search for a tag, manage tags, or create a new tag.

For more information, see [Assign Tags to Ports, on page 95](#).

Step 6 (Optional) To manage the port, click the **Port Actions** drop-down list and choose from the following options:

- To shut down the port and change the port's admin status to Down, choose **Port Shut**. Then click **Okay** to confirm. This option is only available when the port is open and the admin status is Up.
- To open the port and change the port's admin status to Up, choose **Port No Shut**. Then click **Okay** to confirm. This option is only available when the port is shut and the admin status is Down.
- To clear the port's MAC address, choose **Clear Mac Address**.
- To activate an error-disabled port, clear the MAC address and shut down the port.

- Note**
- The device software type must be Cisco IOS or Cisco IOS XE to clear the MAC address and shut down a port.
 - For wireless controllers, clearing the MAC address and shutting down the port are not supported.
 - Clearing the MAC address and shutting down the port are supported only on access ports.
 - Port shutdown disrupts the traffic on a port.

Step 7 To edit certain port details, such as the port description area, use the following table.

Name	Description
Access VLAN	Click the Edit icon. In the Edit Access VLAN dialog box, choose an access VLAN from the drop-down list, and then click Save to assign the access VLAN to the port. You cannot update the access VLAN for the ports that have two access VLANs preconfigured.
Voice VLAN	Click the Edit icon next to Voice VLAN . In the Edit Voice VLAN dialog box, choose a voice VLAN from the Select Value drop-down list, and then click Save to assign the voice VLAN to the port.
Port Description	Click the Edit icon next to PORT DESCRIPTION , enter a description, click Save , and then click Okay to add a description to the port. Click the delete icon to delete the description. In the Warning dialog box, click Okay .

- Note**
- The device software type must be Cisco IOS or Cisco IOS-XE to edit VLAN details and the port description.
 - Editing VLAN details is supported only on access ports.
 - For wireless controllers, editing VLAN details is not supported.

Inventory User Interface Enhancement

The enhanced Cisco DNA Center inventory user interface provides the existing inventory features while improving filters and layout for a better user experience.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The enhanced **Inventory** window appears by default and displays the device information gathered during the discovery process.
- Step 2** Click the location option in the top menu bar to select the site, building, or floor from the network hierarchy to manage your device.
- Step 3** Use the device families area appears at the top of the **Inventory** window to select one or more device families.
The available device families are: **Routers**, **Switches**, **Wireless Controllers**, **Access Points**, and **Sensors**.
- Step 4** Use the **Focus** drop-down list to filter the devices based on **Inventory**, **Default**, **Software Image**, **Provision**, **Security**, or **Device Replacement**.
- Step 5** Use the divider bar at the left corner of the **Device** table to collapse or expand the table width.

- Step 6** In the **DEVICE WORK ITEMS** area, select one or more filter criteria to narrow down the devices in the table.
- Step 7** Click **Add Device** to add a new device in the inventory. For more information, see [Add a Device to a Site](#).
- Step 8** Use **Tag** to tag a device. For more information, see [Manage Devices in Inventory, on page 90](#).
- Step 9** Use the **Action** drop-down list to perform the device actions on one or more devices.
- Step 10** Click the **i** icon to learn about the list of actions and their respective functionalities.
- Step 11** To edit or customize the inventory table, click the gear icon in the right corner at the top of the table and do the following:
- Click **Table Appearance** to define the **Table Density** and **Table Striping**.
 - Click **Edit Table Columns** to select the device information that you want to include in the inventory table during the discovery process.
 - Click **Edit Custom Views** to customize your current view.
 - Click **Apply** to save the changes or click **Reset All Settings** to apply the default settings for the inventory table.
- Step 12** Use the **Filter Devices** option to apply the advanced filter in your device table. For more information, see [Filter Devices](#).
- Step 13** Click the toggle buttons at the top-right corner to switch between **Dashboard**, **Table**, **Topology**, and **Map** view.
- Step 14** Click **Go to old page** to navigate to old inventory window.
- Step 15** Use **Export** to export all data in the device table.
-

Manage User-Defined Fields

User-defined fields are custom labels that you can create and assign to any device in Cisco DNA Center. These labels allow you to display more details about the device. For a user-defined field to be displayed, you must assign it to a device and add a value to it.

Create User-Defined Fields

Cisco DNA Center allows you to create user-defined fields and assign them to any device.

- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- The **Inventory** window displays the device information that is gathered during the discovery process.
- Step 2** From the **Actions** drop-down list, choose **Provision > Inventory > Manage User Defined Fields**.
- Step 3** In the **Manage User Defined Fields** slide-in pane, click **Create New Field**.
- Step 4** In the **Create New Field** dialog box, enter a name and description in the **Field Name** and **Field Description** fields.
- Note** You can add device details that are not already present in the **Device Details** window, such as customer IP address and customer device name, in user-defined fields.
- Step 5** Click **Save**.
- Similarly, you can create more user-defined fields. These fields are displayed in a table.
- Step 6** (Optional) To edit a user-defined field, click the corresponding edit icon, make the required changes, and click **Save**.

- Step 7** (Optional) To delete a user-defined field, click the corresponding delete icon and click **Yes** in the subsequent warning message.

Add User-Defined Fields to a Device


Before you begin

You must have created at least one user-defined field in the **Manage User Defined Fields** window. See [Create User-Defined Fields, on page 71](#).

- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window displays the device information that is gathered during the discovery process.
- Step 2** Click the name of the device for which you want to add user-defined fields.
- Step 3** In the left pane, click **User Defined Fields**.
- Step 4** Click **Add**.
- Step 5** From the **Field Name** drop-down list, choose a user-defined field and enter its value in the **Value** field.
For example, if you created a user-defined field for the customer IP address, choose it from the **Field Name** drop-down list, and enter the customer IP address in the **Value** field.
- Step 6** (Optional) To remove a user-defined field from the device, click the corresponding delete icon.
- Step 7** Click **Save**.

Launch Topology Map from Inventory

You can launch the Topology map for the discovered devices from the **Inventory** window.

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** Use the Toggle button () to switch between the Topology map view and the Inventory view. The Topology map view displays the topology and the provisioning status of the device. Click on each node to view the device details. See [About Topology, on page 115](#) for more information on Topology map.

Note Click **Collapse All** or **Expand All** to collapse and expand the Topology map view.

Types of Devices in the Cisco DNA Center Inventory

Devices show up in inventory one of two ways: by being discovered or by being added manually. Cisco DNA Center Inventory supports the following types of devices:

- **Network Devices:** Supported network devices include Cisco routers, switches, and wireless devices such as wireless controllers and access points (APs).
- **Compute Devices:** Supported compute devices include the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.
- **Meraki Dashboard:** Dashboard to the Cisco cloud management platform for managing Cisco Meraki products.
- **Firepower Management Center (FMC):** Provides complete and unified management over Firepower Threat Defense (FTD) devices for managing Cisco network security solutions.

For a complete list of supported devices, see the [Cisco DNA Center Compatibility Matrix](#).

Manage Network Devices

Add a Network Device

You can add a network device to your inventory manually.

Before you begin

Make sure you configure your network device. For more information, see [Discovery Prerequisites, on page 38](#).

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Click **Add Device**.

Step 3 From the **Type** drop-down list, choose **Network Device**.

Step 4 In the **Device IP / DNS Name** field, enter the IP address or name of the device.

Note If the device uses HSRP protocol, you must enter the primary IP address and not the virtual IP address.

Step 5 Expand the **CLI** area, if it is not already expanded, and do one of the following:

a) To use global credentials, click the **Select global credential** radio button.

Note If no CLI global credentials are available, create the global CLI credentials in the **Network Settings > Device Credentials** window. See [Configure Global CLI Credentials, on page 194](#).

b) To configure credentials for the specific device, click the **Add device specific credential** radio button and configure the following fields:

Table 12: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials. If authentication fails for CLI, Cisco DNA Center retries the authentication process for 300 seconds (5 minutes).

Field	Description
Username	Name that is used to log in to the CLI of the devices in your network.
Password	<p>Password that is used to log in to the CLI of the devices in your network.</p> <p>For security reasons, re-enter the password as confirmation.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Enable Password	<p>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</p> <p>For security reasons, re-enter the enable password.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

Step 6 Expand the **SNMP** area, if it is not already visible and do one of the following:

- a) To use global credentials, click the **Select global credential** radio button.

Note If no SNMP global credentials are available, create the global SNMP credentials in the **Network Settings > Device Credentials** window. See [Configure Global SNMPv2c Credentials, on page 195](#) and [Configure Global SNMPv3 Credentials, on page 195](#).

- b) Click the **Add device specific credential** radio button and do the following:

Step 7 From the **Version** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

If you choose **V2C**, configure the following fields:

Table 13: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Read Community: Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Write Community: Write community string used to make changes to the SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

If you choose **V3**, configure the following fields:

Table 14: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select Authentication and Privacy as Mode .) Choose one of the following privacy types: <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 8 Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and configure the following fields:

Table 15: SNMP Properties

Field	Description
Retries	Number of times Cisco DNA Center tries to communicate with network devices using SNMP.
Timeout (in Seconds)	Amount of time, in seconds, between retries.

Step 9 Expand the **HTTP(S)** area, if it is not already visible, and do one of the following:

- Click the **Select global credential** radio button if you want to use the global HTTP(S) credentials that have been already created.

Note If no HTTP(S) global credentials are available, create the global HTTP(S) credentials in the **Network Settings > Device Credentials** window. See [Configure Global HTTPS Credentials](#).

- Click the **Add device specific credential** radio button and configure the following fields:

Table 16: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .

Field	Description
Read	<p>You can configure up to 10 HTTPS read credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>
Write	<p>You can configure up to 10 HTTPS write credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>

Step 10 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.

Note NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Table 17: NETCONF Setting

Field	Description
Port	<p>Port on the device. You can use one of the following ports:</p> <ul style="list-style-type: none"> • Port 830 (default). • Any other port that is available on the device. • A custom port that Cisco DNA Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the Cisco DNA Center Administrator Guide.) <p>If authentication fails for NETCONF, Cisco DNA Center retries the authentication process for 300 seconds (5 minutes).</p>

- Step 11** Select one of the network **Protocol** radio button that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.
- Step 12** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.
- All the credentials will be validated except the SNMP Write credentials.
- Step 13** Click **Add**.

Update Network Device Credentials

You can update the discovery credentials of selected network devices. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- The **Inventory** window displays the device information gathered during the discovery process.
- Step 2** Select the network devices that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
- Step 4** In the **Edit Device** dialog box, choose **Network Device** from the **Type** drop-down field, if it is not already selected.
- Step 5** Expand the **CLI** area, if it is not already expanded, and do one of the following:
- If you want to use the global CLI credentials that have been already created, click the **Select global credential** radio button.
- Note** If no CLI global credentials are available, create them in the **Network Settings > Device Credentials** window. See [Configure Global CLI Credentials](#).

- b) Click the **Edit device specific credential** radio button and configure the following fields:

Table 18: CLI Credentials

Field	Description
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password that is used to move to a higher privilege level in the CLI. For security reasons, re-enter the enable password. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 6 Expand the **SNMP** area, if it is not already expanded, and do one of the following:

- a) If you want to use the global SNMP credentials that have been already created, click the **Select global credential** radio button.

Note If no SNMP global credentials are available, create them in the **Network Settings > Device Credentials** window. See [Configure Global SNMPv2c Credentials](#) and [Configure Global SNMPv3 Credentials](#).

- b) Click the **Edit device specific credential** radio button and do the following:

Step 7 From the **Version** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

If you chose **V2C**, configure the following fields:

Table 19: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Read Community: Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Write Community: Write community string used to make changes to the SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

If you chose **V3**, configure the following fields:

Table 20: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select Authentication and Privacy as Mode .) Choose one of the following privacy types: <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 8 Expand the **SNMP RETRIES AND TIMEOUT** area, if it is not already expanded, and configure the following fields.

Table 21: SNMP Properties

Field	Description
Retries	Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3.
Timeout	Number of seconds Cisco DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

Step 9 Expand the **HTTP(S)** area, if it is not already expanded, and do one of the following:

- If you want to use the global HTTP(S) credentials that have been already created, click the **Select global credential** radio button.

Note If no HTTP(S) global credentials are available, create them in the **Network Settings > Device Credentials** window. See [Configure Global HTTPS Credentials](#).

- Click the **Edit device specific credential** radio button and configure the following fields:

Table 22: HTTP(S)

Field	Description
Username	Name that is used to log in to the HTTP(S) of the devices in your network.
Password	<p>Password that is used to log in to the HTTP(S) of the devices in your network.</p> <p>For security reasons, re-enter the password as confirmation.</p> <p>Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Port	Specify the required HTTP(s) port number.

Step 10 Expand the **NETCONF** area, if it is not already expanded, and configure the **Port** field.

NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

- Step 11** Select one of the network **Protocol** radio buttons that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.
- Step 12** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows the valid credentials with green tick mark and invalid credentials with red cross mark.
- If you have chosen more than one device for updating the credentials, the **Validation** button will be disabled.
- Step 13** Click **Update**.
-

Security Focus for Network Devices

The Cisco DNA Center security focus allows you to view the results of the trustworthy checks on your devices.

Few security checks are performed to ensure that your Cisco devices are authentic and are not compromised or altered physically.

As a part of device identity verification, following checks are performed:

- Verification of Secure Unique Device Identifier (SUDI) certificate chain.
- Signature verification of SUDI certificate response of the device.
- Product ID verification with the SUDI certificate.
- Serial number verification with the SUDI certificate.

These checks are triggered under the following circumstances:



- Every time Inventory gets collected in the Cisco DNA Center.
- When you make any configuration changes on your devices.
- When you make any image upgrades in your devices.

The following CLI command is used to perform device identity verification check:

```
show platform sudi certificate sign nonce ${randomNonceValue}
```

View the Integrity Verification Status of a Device

This procedure explains how to view the status of the integrity verification check.

- Step 1** Click the menu icon () and choose **Provision > Inventory**.
- The **Inventory** window displays the device information that is gathered during the discovery process.
- Step 2** From the **Focus** drop-down menu, choose **Security**.
- Step 3** In the **Devices** table, if the **Integrity Verification** column for your device displays **Failed** as the status, click the information icon () to display the reason.
- Note** If the **Integrity Verification** column is not displayed, see [Display Information About Your Inventory, on page 57](#).
-

Manage Compute Devices

Add a Compute Device

You can add a compute device to your inventory manually. A compute device includes devices such as the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Click **Add Device**.

Step 3 From the **Type** drop-down list, choose **Compute Device**.

Step 4 In the **Device IP / DNS Name** field, enter the IP address or name of the device.

Step 5 Expand the **HTTP(S)** area, if it is not already expanded, and do one of the following:

- a) If you want to use the global HTTP(S) credentials that have been already created, click the **Select global credential** radio button.

Note If no HTTP(S) global credentials are available, create them in the **Network Settings > Device Credentials** window. See [Configure Global HTTPS Credentials, on page 197](#).

- b) Click the **Add device specific credential** radio button and configure the following fields:

Table 23: HTTP(S)

Field	Description
Username	Name used to authenticate the HTTPS connection.
Password	Password used to authenticate the HTTPS connection.
Port	Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

Step 6 Expand the **CLI** area, if it is not already expanded, and do one of the following:

- a) If you want to use the global CLI credentials that have been already created, click the **Select global credential** radio button.

Note If no CLI global credentials are available, create them in the **Network Settings > Device Credentials** window. See [Configure Global CLI Credentials, on page 194](#).

- b) Click the **Add device specific credential** radio button and configure the following fields:

Table 24: CLI Credentials

Field	Description
Username	Name that is used to log in to the CLI of the devices in your network.

Field	Description
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, re-enter the password as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.
Enable Password	Password that is used to move to a higher privilege level in the CLI. For security reasons, re-enter the enable password. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 7 Expand the **SNMP** area, if it is not already expanded, and do one of the following:

- a) If you want to use the global SNMP credentials that have been already created, click the **Select global credential** radio button.

Note If no SNMP global credentials are available, create them in the **Network Settings > Device Credentials** page. See [Configure Global SNMPv2c Credentials, on page 195](#) and [Configure Global SNMPv3 Credentials, on page 195](#).

- b) Click the **Add device specific credential** radio button and do the following:

Step 8 From the **Version** drop-down list, choose **V2C** (SNMP Version 2c) or **V3** (SNMP Version 3).

If you chose **V2C**, configure the following fields:

Table 25: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Read Community: Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Write Community: Write community string used to make changes to the SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

If you chose **V3**, configure the following fields:

Table 26: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • Authentication and Privacy: Provides both authentication and encryption. • Authentication, No Privacy: Provides authentication, but does not provide encryption. • No Authentication, No Privacy: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select Authentication and Privacy or Authentication, No Privacy as Mode .) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA. • MD5 (not recommended): Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select Authentication and Privacy as Mode .) Choose one of the following privacy types: <ul style="list-style-type: none"> • AES128: 128-bit CBC mode AES for encryption. • CISCOAES192: 192-bit CBC mode AES for encryption on Cisco devices. • CISCOAES256: 256-bit CBC mode AES for encryption on Cisco devices. <p>Note</p> <ul style="list-style-type: none"> • Privacy types CISCOAES192 and CISCOAES256 are supported only for use with Discovery and Inventory features. Assurance features are not supported. • Privacy type AES128 is supported for Discovery, Inventory, and Assurance.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 9 (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows the valid credentials with green tick mark and invalid credentials with red cross mark.

All the credentials will be validated except the SNMP Write credentials.

Step 10 Click **Add**.

Update Compute Device Credentials

You can update the discovery credentials of selected compute devices. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon () and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Select the devices that you want to update.

Step 3 From the **Actions** drop-down list, choose **Inventory > Edit Device**.

Step 4 In the **Edit Device** dialog box, from the **Type** drop-down list, choose **Compute Device**.

Step 5 Expand the **HTTP(S)** area, if it is not already expanded.

Step 6 In the **Username** and **Password** fields, enter the username and password.

Step 7 In the **Port** field, enter the port number.

Step 8 (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.

If you have chosen more than one device for updating the credentials, the **Validation** button is disabled.

Step 9 Click **Update**.

Manage Meraki Dashboards

Integrate the Meraki Dashboard

You can integrate your Meraki dashboard with Cisco DNA Center.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The **Inventory** window displays the device information that is gathered during the discovery process.
- Step 2** Click **Add Device**.
- Step 3** In the **Add Device** dialog box, from the **Type** drop-down list, choose **Meraki Dashboard**.
- Step 4** Expand the **HTTP(S)** area, if it is not already expanded.
- Step 5** In the **API Key/Password** field, enter the API key and password credentials and click the **Get Organization details** link.
- Step 6** From the **Organization** drop-down list, select the organization options, or search for an organization name.
- Step 7** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.
- Step 8** Click **Add**.
Only the selected organizations start collecting for the Meraki dashboard and devices.
-

Update Meraki Dashboard Credentials

You can update the Meraki dashboard credentials of selected devices. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The **Inventory** window displays the device information that is gathered during the discovery process.
- Step 2** Select the devices that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
- Step 4** In the **Edit Device** slide-in pane, from the **Type** drop-down list, choose **Meraki Dashboard**.
- Step 5** Expand the **HTTP(S)** area, if it is not already expanded.
- Step 6** In the **API Key / Password** field, enter the API key and password credentials used to access the Meraki dashboard.
- Step 7** In the **Port** field, enter the port number.
- Step 8** (Optional) Click **Validate** next to **Credentials**. Cisco DNA Center validates the device credentials and shows valid credentials with a green tick mark and invalid credentials with a red cross mark.
If you have chosen more than one device for updating the credentials, the **Validation** button is disabled.

Step 9 Click **Update**.

Manage Firepower Management Center

Integrate Firepower Management Center

You can integrate your Firepower Management Center (FMC) with Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Click **Add Device**.

Step 3 In the **Add Device** dialog box, from the **Type** drop-down list, choose **Firepower Management Center**.

Step 4 In the **Device IP / DNS Name** field, enter the IP address or name of the device.

Step 5 Expand the HTTP(S) area if it is not already expanded.

The **Add device specific credential** radio button is chosen by default.

Step 6 Enter the following information:

- a) **Username:** Name used to authenticate the HTTPS connection.
- b) **Password:** Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration.
- c) **Port:** The number of the TCP/UDP port used for HTTPS traffic. The default port number is 443.

Step 7 Click **Add**.

Note When you add FMC to inventory, the Firepower Threat Defense (FTD) devices managed by FMC are also added to inventory automatically.

Update Firepower Management Center Credentials

Cisco DNA Center allows you to update the Firepower Management Center (FMC) credentials. The updated settings override the global and job-specific settings for the selected devices.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Choose the FMC device that you want to update.

Note You cannot update, edit, or delete the Firepower Threat Defense (FTD) devices that are managed by FMC. You must manage FTD devices via FMC in inventory.

- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
- Step 4** In the **Edit Device** slide-in pane, click **Credentials**.
- Step 5** Expand the HTTP(S) area if it is not already expanded.
The **Add device specific credential** radio button is chosen by default.
- Step 6** Enter the following information:
- Username:** Name used to authenticate the HTTPS connection.
 - Password:** Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration.
 - Port:** The number of the TCP/UDP port used for HTTPS traffic. The default port number is 443.
- Step 7** Click **Management IP** and enter the IP address or name of the device in the **Device IP / DNS Name** field.
- Step 8** Click **Resync Interval** and choose a resync interval type:
- **Custom:** You can enter the resync interval in minutes. The valid ranges are from 25 to 1440 minutes (24 hours).
 - **Global:** By default, resync interval is set to 1440 minutes (24 hours).
 - **Disable:** Resync interval is disabled or set to zero.
- Step 9** Click **Role** and choose a role in the **Device Role** drop-down list.
- Step 10** Click **Update**.

Filter Devices

In the **Inventory** window, you can choose from basic or advanced filtering options to filter for device details in the **Devices** table.

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The **Inventory** window displays the device information that is gathered during the discovery process.
- Step 2** Click **Filter devices**.
The following table describes the available filtering options.

Name	Description
Quick Filters	You can choose from basic filtering options to narrow down the device details. For example, you can toggle the Manageability filter option to Managed to see all the managed devices.
Advanced Filters	You can set the filtering criteria using operators, such as Contains and Regex (Regular Expression), to narrow down the device details. For example, in the Tags drop-down list, you can choose the Contains operator and enter ipsec in the Tags field. Then from the autocomplete drop-down list, you can choose one option, such as branch-router-ipsec , which would filter for branch routers that are tagged with IP Security. You must enter filter criteria values based on the available data.

Name	Description
Recent Filters	In the RECENT area, you can choose a recent filter to reapply. To save a recent filter, drag and drop a recent filter to the SAVED area.

Step 3 Choose a filtering option and enter the appropriate value in the selected filter field.

Cisco DNA Center presents you with autocomplete values as you enter values in the other fields. Choose one of the suggested values or finish entering the wanted value.

You can also use a wildcard (asterisk) with these filters. For example, you can enter values with an asterisk at the beginning, end, or in the middle of a string value. Then, press **Enter**.

Step 4 Click **Apply** to filter the information.

The data displayed in the **Devices** table updates automatically according to your filter selection.

Note You can use several filter types and more than one value per filter.

Step 5 (Optional) If needed, add more filters.

Step 6 (Optional) To remove all the filters, in the **Filter devices** field, click the **x** and then click **Apply**.

Step 7 (Optional) To delete a specific filter value, in the **Filter devices** field, drag your cursor over the value, press **Delete**, and then click **Apply**.

Manage Devices in Inventory

The following sections provide information about how to assign devices to sites and manage device tags by using the **Inventory** window.


Add a Device to a Site

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Check the check box for the devices that you want to assign to a site.

Step 3 From the **Actions** menu, choose **Provision > Assign Device to Site**.

Step 4 In the **Assign Device to Site** slide-in pane, click the link next to the  icon for the device.

Step 5 In the **Choose a floor** slide-in pane, select the floor to assign to the device and click **Save**.

Step 6 (Optional) If you select multiple devices to add to the same location, check the **Apply to All** check box for the first device to assign its location to the rest of the devices and click **Next**.

Step 7 Check **Application and Endpoint Visibility is enabled on all applicable devices. Check this to skip enabling it on all devices** check box.

Note **Application and Endpoint Visibility** enablement is skipped by default for the devices that does not support Controller-Based Application Recognition (CBAR) enablement or undeployed Application Visibility Service (AVS).

- Step 8** Review summary settings and click **Next**.
- Step 9** In the **Task Name** name field, enter a task name of your choice.
- Step 10** Choose whether you want to assign the device to a site **Now** or schedule it for later.
- Step 11** Click **Assign**.
- Step 12** To preview the CLI configuration, click the **Generate Configuration Preview** radio button and do the following:
- In the **Task Name** name field, enter a task name of your choice and click **Preview**.
Later, you can use the created configuration preview to deploy to the selected devices.
 - In the **Task Submitted** dialog box, click the **Work Items** link.
Note This dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon (≡) and choose **Activities > Work Items**.
 - In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
 - View the CLI configuration details and click **Deploy**.
 - To immediately deploy the device, click the **Now** radio button, and click **Apply**.
 - To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
 - In the confirmation window, click **Yes**.
Note The CLI task is marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.
- Step 13** When assigning devices to a site, if Device Controllability is enabled, a workflow is automatically triggered to push the device configuration from the site to the devices.
From the **Focus** drop-down list, choose **Provision** and click **See Details** in the **Provision Status** column. The configuration that is pushed to the device is shown in a separate window if you enabled Device Controllability.
-

Tag Devices

A device tag allows you to group devices based on an attribute or a rule. A single device can have multiple tags; similarly, a single tag can be applied to multiple devices.

You can add tags to or remove tags from devices in the **Inventory** window.


- Step 1** Click the menu icon (≡) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.
- Step 2** Check the check box next to the device(s) for which you want to apply a tag, and then click **Tag**.
- Step 3** Enter a tag name in the **Tag Name** field.
- If you are creating a new tag, click **Create New Tag**. You also can create a new tag with a rule. See [Tag Devices Using Rules, on page 92](#).
 - If you are using an existing tag, select the tag from the list, and then click **Apply**.

A tag icon and the tag name(s) appear under the device name(s) for which you applied the tag(s).

- Step 4** To remove a tag from a device, do one of the following:
- Click **Create New Tag**, unselect all tags, and then click **Apply**.
 - Hover the cursor over the tag icon or tag name, and then click **X** to disassociate the tag from the device.

Tag Devices Using Rules

You can group devices based on tags in which you define a rule. When you define a rule, Cisco DNA Center automatically applies the tag to all devices that match the specified rule. Rules can be based on device name, device family, device series, IP address, location, or version.


- Step 1** Click the menu icon () and choose **Provision > Network Devices > Inventory**. The **Inventory** window displays the device information gathered during the discovery process.
- Step 2** Check the check box next to the device(s) for which you want to apply a tag, then click **Tag**.
- Step 3** Enter a tag name in the **Tag Name** field, then click **Create New Tag with Rule**. The **Create New Tag** window appears. The **Manually Added** field under **Total Devices Tagged Count** indicates the number of devices you selected.
- Step 4** Click **Add Condition**, then complete the required fields for the rule. The **Matching Devices** number automatically changes to indicate how many devices match this condition. You can have two options to create additional conditions:
- *And* conditions: Click the **Add Condition** link. **And** appears above the condition.
 - *Or* conditions: Click the add icon (+) next to an existing condition. **Or** appears next to the condition.

You can add as many conditions as needed. As you make changes to the rule, the Matching Devices count changes to reflect how many devices in the inventory match the rule you specified. You can click on the device number to view the devices that match the rule.

- Step 5** Click **Save** to save your tag with the defined rule. A tag icon and the tag name(s) appear under the device name(s) for which you applied the tag(s). As devices are added to the inventory, if they match the rules you defined, the tag is automatically applied to the devices.

Edit Device Tags

You can edit device tags that you previously created.

- Step 1** Click the menu icon () and choose **Provision > Network Devices > Inventory**.

The **Inventory** window displays device information gathered during the discovery process.

In the **Device Name** column, you can see any previously created device tags listed under the device names.

Step 2 Without selecting any devices, click **Tag**.

The previously created tags are listed.

Step 3 Click **Manage Tags**.

The **All Tags** slide-in pane is displayed.

Step 4 Click the pencil icon next to the tag that you want to edit.

Step 5 Make changes to the tag, then click **Save**.

Delete Tags

You can delete a device tag or template tag only if it is not associated with a device or template.

Before you begin

Remove the tag that is associated statically or dynamically (using rules) with the device.

Remove the tag that is associated with a template.

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Without selecting any devices, choose **Tag > Manage Tags**.

Step 3 Hover your cursor over the tag that you want to delete, then click the delete icon next to the tag name.

Step 4 At the prompt, click **Yes**.

An error message is generated if the tag is associated with a device or template. Remove the tag associated with the device or template and delete the tag.

Configure a REP Ring for Devices

The Resilient Ethernet Protocol (REP) ring provides a way to control network loops, handle link failures, and improve convergence time.



Note

- Limitation of a REP Ring: You should not select a root node that has connectivity only through interfaces of the ring.
 - Device support for REP Ring (nonfabric): Cisco Catalyst Industrial Ethernet Series Switch 3200, 3300, 3400, 4000, and 5000. Cisco Embedded Services 3300 Series Switches (ESS3300), and S5800.
-

Before you begin


- Make sure the devices are onboarded and are in reachable state.
- Identify the devices and its interfaces that terminate the REP ring.
- Make sure all the interfaces which are part of the ring are configured with “switchport mode trunk”.

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure REP Ring (Non-Fabric)**.
Alternatively, you can navigate to the **Inventory Site** topology view, select the device node on which you want to create the REP ring, and click **Create REP Ring** under the **REP Rings** tab.
- Step 2** If a task overview window appears, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Select a root device** window, select the root device.
Note The device must be in reachable state and have upstream connection.
- Step 4** In the **Select adjacent devices connected to root device** window, choose one adjacent device that is part of the ring and connected to the root device.
- Step 5** In the **Select adjacent devices connected to root device** window, choose other adjacent device that is part of the same ring and connected to the root device.
You need to choose two devices, part of the same ring and directly connected to the root device.
- Step 6** **Review** and **Edit** your root device, and the chosen adjacent devices.
- Step 7** To initiate the REP ring configuration, click **Provision**.
You can see a detailed status of the configuration progress on the **REP Ring Configuration Status** window.
- Step 8** The **REP Ring Summary** window displays the details of the REP ring that is created along with the discovered devices. After the creation of the REP ring, a success message is displayed.
- Step 9** To verify the creation of the REP ring, go to the **Inventory** window topology view and click any device that is part of the ring. In the slide-in pane, under the **REP Rings** tab, you can see the list of all REP rings that exist on that device.
Click a REP ring name in the list to view the REP ring details, such as the devices present in the ring, ports of each device that connect to the ring, and so on.
-

Create Port Groups


You can group ports based on an attribute or rule.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The **Inventory** window displays device information gathered during the discovery process.
- Step 2** To create a new port tag, click **Tag** and choose **Create New Tag**.
The **Create New Tag** slide-in pane is displayed.

- Step 3** In the **Tag Name** field, enter the tag name. In the **Description** field, add a description for the tag.
- Note** The **WAN** tag is a reserved tag name. You can't create a new port tag named **WAN**, because the system autogenerates the **WAN** tag.
- Step 4** In the **Tag Rules** area, click the **Port** tab.
- Step 5** In the **Device Scope** area, click the drop-down list and choose **Location** or **Tag Name** of the device to define the filters.
- Step 6** To add rules for tagging the ports, click the  icon. You can tag the ports based on port status, speed, tag name, operational status, and description. You can add additional conditions using Boolean operators (AND, OR).
- To delete a condition, click the delete icon.
- Step 7** As the conditions are set, you can find the link for ports matching the condition at the bottom-left corner of the pane.
- Click the link to view the ports. In the **Matching Ports** slide-in pane, you can view the device to which the port belongs and the port name.
- Step 8** Click **Save**.
-


Assign Tags to Ports

You can manually assign tags to ports. For example, you can manually assign the system-generated **WAN** tag to a port.

- Step 1** Click the menu icon () and choose **Provision > Inventory**.
- Step 2** In the **Inventory** window, click a device name and choose **View Device Details**.
- Step 3** In the left pane, expand **Interfaces** and click **Ethernet Ports**.
- Step 4** In the top-right corner of the window, switch to the table view.
- Step 5** Choose the port or ports to tag and click **Tag**.
- Step 6** Choose the appropriate tags.
- Step 7** Click **Apply**.
-

Port Usage Information

You can check the last input received and last output sent by the port.

- Step 1** Click the menu icon () and choose **Provision > Inventory**.
- Step 2** In the **Devices** table, click a device name, and then click **View Device Details**.
- The device details are displayed in the window.
- Step 3** In the left pane, choose **Interfaces > Ethernet Ports**.

Note This tab is available for all devices except APs.

Step 4 Click the port to view its details.

In the window, you can view the timestamp of **Last Input** received by the port and **Last Output** transmitted by the port.

Maintenance Mode for Devices

Schedule Maintenance for Devices

You can place one or more devices under maintenance mode in Cisco DNA Center. If a device is placed under maintenance mode, Cisco DNA Center will not process any telemetry data associated with the device. By placing faulty devices under maintenance mode, you can avoid receiving unnecessary alerts from the devices.



Note From the devices in maintenance mode, you cannot collect any information and perform polling operations.

While scheduling the maintenance mode for Cisco Wireless Controllers and APs, note the following:

- When you schedule maintenance for a Cisco Wireless Controller, all the APs associated with the wireless controller are moved under maintenance mode with the same schedule.
- When a wireless controller is in maintenance mode, you cannot modify the maintenance schedule of a single AP associated with the wireless controller. A warning message saying that the device is already scheduled for maintenance is displayed. If you modify the schedule of the wireless controller, then all the APs under the wireless controller will be impacted.
- When an AP moves from one wireless controller to another, the maintenance mode is impacted as below:
 - If the AP is moving from a wireless controller which is in maintenance mode to a wireless controller which is not under maintenance, then the AP will not have maintenance mode after moving.
 - If the AP is moving from a wireless controller which is not in maintenance mode to a wireless controller which is under maintenance, then the AP will be in maintenance mode after moving.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Choose the devices that you want to schedule maintenance.

Step 3 From the **Actions** drop-down list, choose **Inventory > Schedule Maintenance**.

The **Schedule Maintenance** slide-in pane is displayed.

Step 4 In the **Reason For Maintenance** field, enter a reason for placing the device under maintenance mode.

By default, Cisco DNA Center adds a reason, and you can modify it.

- Step 5** In the **Define Maintenance Window** area, do the following:
- Choose the start date and time for maintenance.
 - Choose the end date and time for maintenance.
 - Alternately, click **Days/Hours** and enter days and hours for maintenance.
- Note:** To choose recurrence for maintenance, choose **Days/Hours** option.
- Step 6** In the **Maintenance Recurrence** area, click **None**, **Daily**, or **Weekly**.
- **None:** Maintenance will not recur.
 - **Daily:** Enter the interval in days in the **Run at Interval (Days)** field.
 - **Weekly:** Enter the interval in weeks in the **Run at Interval (Weeks)** field.
- Step 7** If you have chosen **Daily** or **Weekly** for recurrence, check the **Set Schedule End** check box.
- Step 8** Click **End Date** or **End After (Occurrences)**.
- **End Date:** Enter month, date, and year for maintenance end.
 - **End After (Occurrences):** Enter the number of occurrences after you want maintenance to end.
- Step 9** In the **Maintenance Time Zone** area, choose time zone for maintenance.
- Step 10** Click **Submit**.
-

Manage Maintenance Schedule for Devices

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** From the **Actions** drop-down list, choose **Inventory > Manage Maintenance**.
- The **Manage Maintenance** slide-in pane is displayed. The **Status** column shows the current status of maintenance schedules.
- Step 3** Click the **Search** or **Filter** icon to search or filter maintenance schedules.
- Step 4** In the **Actions** column, click the **Edit** icon to edit the maintenance schedule.
- Note** For in-progress maintenance schedules, you can only extend the maintenance end time.
- Step 5** Click the **Delete** icon in the **Actions** column to delete the maintenance schedule.
- Note** You cannot delete in-progress maintenance schedules.
-

Inventory Insights

The **Inventory Insights** window displays devices that have configuration inconsistencies with other directly-connected devices. It also displays devices that are misconfigured, as compared with the Cisco DNA

Center best-practice recommendations. Additionally, you can view whether the link between the devices is up (active) or down (inactive), a link is down when the connection between devices no longer exists. Historical data is retained for future reference.

For example, assume that there is a network link between *device A* and *device B*. If you remove the link from *device B* and connect it to a new *device C*:

- The old link between *device A* and *device B* remains present and can be manually deleted by the user from the **Tools > Topology** window. No action is required by the user on the **Inventory Insights** window, it is shown to retain the historical data for your reference.
- The new link between *device A* and *device C* is shown as up.

Cisco DNA Center provides below insights with suggested actions.

Speed/Duplex Settings Mismatch

Cisco DNA Center displays the devices that are connected with each other but configured with different speed and duplex values at the two ends of a device link.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory Insights**.
The **Inventory Insights** window appears.
- Step 2** Click **Speed/Duplex settings mismatch** to see the suggested actions that can be performed on devices.
The suggested actions appear in the right pane.
- Step 3** Click the number of instances to see the mismatches.
The **Speed/Duplex settings mismatch** window highlights the mismatches of speed and duplex.
- Step 4** Make the required changes in the device configuration by following the suggested actions.
-

VLAN Mismatch

Cisco DNA Center displays the devices that are connected with each other but configured with different VLANs at the two ends of a device link.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory Insights**.
The **Inventory Insights** window appears.
- Step 2** Click **VLAN Mismatch** to see the suggested actions that can be performed on devices.
The suggested actions appear in the right pane.
- Step 3** Click the number of instances to see the mismatches.
- Step 4** Make the required changes in the device configuration by following the suggested actions.
-

Manage System Beacon

You can highlight switches in the Cisco DNA Center inventory by using system beacons.

You can enable a system beacon on the following devices:

- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 3850 Series Ethernet Stackable Switches

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Choose the devices for which you want to enable or disable beacons.

Note

- You can enable beacons on up to five standalone devices at a time.
- To enable beacons on stacked devices, you must choose only one device at a time. In a stacked device, you can enable beacons on one or more stack members.

Step 3 From the **Actions** drop-down list, choose **Inventory > Manage System Beacon**.

Step 4 In the **Manage System Beacon** slide-in pane, click the **Enabled** radio button under **System Beacon State** and then click **Apply** to enable a beacon on the chosen devices.

After the system beacon is enabled, a blue beacon icon (📶) is displayed next to the device name in the inventory.

Step 5 (Optional) If you have chosen a stacked device, do the following in the **Manage System Beacon** slide-in pane:

- a) Check the **Update System Beacon Status?** check box corresponding to the stack members that you want to enable beacon.
- b) Under **System Beacon State**, click the **Enabled** radio button.
- c) Click **Apply**.

Step 6 (Optional) To disable a beacon on the chosen devices, do the following in the **Manage System Beacon** slide-in pane:

- a) Under **System Beacon State**, click the **Disabled** radio button.
- b) Click **Apply**.

Alternatively, in the **Inventory** window, hover the cursor over the blue beacon icon (📶) next to the device name and click **Disable**.

Change the Device Role (Inventory)

During the discovery process, Cisco DNA Center assigns a role to each of the discovered devices. Device roles are used to identify and group devices and to determine a device's placement on the network topology map in the Topology tool. The top tier is the internet. The devices underneath are assigned one of the following roles:

Table 27: Device Roles and Topology Positions

Topology Position	Device Role
Tier 1	Internet (not configurable)
Tier 2	Border Router
Tier 3	Core
Tier 4	Distribution
Tier 5	Access
Tier 6	Unknown



Note When you assign the **Access** role to a device, IP Device Tracking (IPDT) is either configured or removed from the device based on the IPDT settings of the Site.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 To update the device role in the **Edit Device** slide-in pane:

- a) Select the device whose role you want to change.
- b) From the **Actions** drop-down list, choose **Inventory > Edit Device**.
- c) Click the **Role** tab and choose an appropriate role from the **Device Role** drop-down list.

Note If you manually change the device role, the assignment remains static. Cisco DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization.

Update a Device's Management IP Address

You can update the management IP address of a device.



Note You cannot update more than one device at a time. Also, you cannot update a Meraki device's management IP address.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The **Inventory** window displays the device information that is gathered during the discovery process.
- Step 2** Select the device that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
The **Edit Device** slide-in pane is displayed.
- Step 4** Click the **Management IP** tab, and enter the new management IP address in the **Device IP/ DNS Name** field.
- Note** Make sure that the new management IP address is reachable from Cisco DNA Center and that the device credentials are correct. Otherwise, the device might enter an unmanaged state.
-

What to do next

Reprovision the device to update the source-interface configuration.

Update the Device Polling Interval

You can update the polling interval at the global level for all devices by choosing **System > Settings > Network Resync Interval** or at the device level for a specific device by choosing **Device Inventory**. When you set the polling interval using the **Network Resync Interval**, that value takes precedence over the **Device Inventory** polling interval value.

If you do not want a device to be polled, you can disable polling.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** Select the devices that you want to update.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Edit Device**.
- Step 4** In the **Edit Device** slide-in pane, click **Resync Interval**.
- Step 5** Select the resync type.
- Note**
- To set the resync type as global, go to **System > Settings**.
 - The device-specific polling time supersedes the global polling time. If you set the device-specific polling time and then change the global polling time, Cisco DNA Center continues to use the device-specific polling time.
- Step 6** In the **Resync Interval (in Mins)** field, enter the time interval (in minutes) between successive polling cycles.

Step 7 Click **Update**.

Resynchronize Device Information

You can immediately resynchronize device information for selected devices, regardless of their resynchronization interval configuration. A maximum of 40 devices can be resynchronized at the same time.

Step 1 Click the menu icon () and choose **Provision > Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Select the devices about which you want to gather information.

Step 3 From the **Actions** drop-down list, choose **Inventory > Resync Device**.

Step 4 Click **OK**.

Delete a Network Device

You can delete devices from the Cisco DNA Center database, as long as they have not already been added to a site.

When you remove a wireless sensor from the inventory, the sensor is reset to the factory defaults so that when it rejoins, it gets the current configuration.

Before you begin

You must have administrator (ROLE_ADMIN) permissions and access to all devices (RBAC Scope set to ALL) to perform this procedure.

Step 1 Click the menu icon () and choose **Provision > Inventory**.

The **Inventory** window displays the device information gathered during the discovery process.

Step 2 Check the check box next to the device or devices that you want to delete.

Note You can select multiple devices by checking additional check boxes, or you can select all the devices by checking the check box at the top of the list.

Step 3 From the **Actions** drop-down list, choose **Inventory > Delete Device**.

Step 4 In the **Warning** window, check the **Config Clean-Up** check box to remove the network settings and telemetry configuration from the selected device.

Step 5 Confirm the action by clicking **OK**.

Launch Command Runner (Inventory)

You can launch the Command Runner application for selected devices from within the **Inventory** window.

Before you begin

Install the Command Runner application. For more information, see the [Cisco DNA Center Administrator Guide](#).

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Select the devices on which you want to run commands.

Step 3 From the **Actions** drop-down list, choose **More > Command Runner**.

For information about the commands that you can run and how to run them, see [Run Diagnostic Commands on Devices, on page 361](#).

Troubleshoot Device Reachability Issues Using Run Commands

You can launch the **Run Commands** window from the **Inventory** window and run platform commands, such as ping, traceroute, and snmpget, to troubleshoot device reachability issues.



Note If you want to execute the platform commands directly on a Cisco DNA Center cluster, do not select any device before launching **Run Commands**. Otherwise, the execution of commands will be for that device and not the platform.

Before you begin

Install the Command Runner application. For more information, see the [Cisco DNA Center Administrator Guide](#).

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

Step 2 From the **Actions** drop-down list, choose **More > Run Commands**.

You can enter **man** anytime to retrieve a list of currently supported commands and shortcuts.

Use a CSV File to Import and Export Device Configurations

CSV File Import

You can use a CSV file to import your device configurations or sites from another source into Cisco DNA Center. If you want to download a sample template, go to the **Inventory** window and choose **Actions > Inventory > Import Inventory**. Click **Download Template** to download a sample CSV file template.

When you use a CSV file to import device or site configurations, the extent to which Cisco DNA Center 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, Cisco DNA Center will have limited functionality and cannot modify device configurations, update device software images, or perform any other valuable functions.

You can specify the credential profile in the CSV file to apply the corresponding credentials to a set of devices. If you specify the credential profile and also enter the values manually in the CSV file, the manually entered credentials take higher priority and the device is managed based on a combination of manually entered credentials and credential profile. For example, if the CSV file contains a credential profile with SNMP and SSH or Telnet credentials in addition to manually entered SNMP credentials, the device is managed based on the manually entered SNMP credentials and the SSH or Telnet credentials in the credential profile. Telnet is not recommended.



Note You also must 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.

For partial inventory collection in Cisco DNA Center, 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 Cisco DNA Center, 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

- CLI username
- CLI password
- CLI enable password
- CLI timeout value

CSV File Export

Cisco DNA Center enables you to create a CSV file that contains all or selected devices in the inventory. When you create this file, you must enter a password to protect the configuration data that the file will contain.

Import Device Configurations from a CSV File

You can import device configurations from a CSV file.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.
- Step 2** From the **Actions** drop-down list, choose **Inventory > Import Inventory** to import the device credentials.
- Step 3** Drag and drop the CSV file into the boxed area in the **Bulk Import** dialog box or click the dotted-line boxed area and browse to the CSV file.
- Step 4** Click **Import**.
-

Export Device Data

You can export specific data pertaining to selected devices to a CSV file. The CSV file is compressed. Click **Export** to export the data of filtered devices or all devices.



Caution Handle the CSV file with care because it contains sensitive information about the exported devices. Ensure that only users with special privileges perform a device export.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.
- Step 2** To export configuration information for only certain devices, check the check box next to the devices that you want to include. To include all devices, check the check box at the top of the device list.
- Step 3** From the **Actions** drop-down list, choose **Inventory > Export Inventory** to export the device configurations.
The **Export Inventory** dialog box appears.
- Step 4** In the **Password** field, enter a password that will be used to encrypt the exported CSV file.
- Note** The password is required to open the exported file.

Step 5 Confirm the encryption password.

Step 6 Check the **Include SSH key information** check box to include information such as initial SSH key, initial SSH key algorithm, current SSH key, and current SSH key algorithm in the exported CSV file.

Step 7 Click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.

Export Device Credentials

You can export device credentials to a CSV file. You are required to configure a password to protect the file from unwanted access. You need to supply the password to the recipient so that the file can be opened.



Caution Handle the CSV file with care because it lists all of the credentials for the exported devices. Ensure that only users with special privileges perform a device export.

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

Step 2 Check the check box next to the devices that you want to include in the CSV file. To include all the devices, select the check box at the top of the list.

Step 3 From the **Actions** drop-down list, choose **Inventory > Export Inventory**.

The **Export** dialog box appears.

Step 4 In **Select Export Type**, click the **Credentials** radio button.

Step 5 Check the **Include SSH key information** check box to include information such as initial SSH key, initial SSH key algorithm, current SSH key, and current SSH key algorithm in the exported CSV file.

Step 6 In the **Password** field, enter a password that will be used to encrypt the exported CSV file.

Note The password is required to open the exported file.

Step 7 Confirm the encryption password and click **Export**.

Note Depending on your browser configuration, you can save or open the compressed file.

Configuration Drift of a Device

Configuration changes made on devices are saved in the internal Cisco DNA Center server. For information on how to view the configuration drift, see [View Configuration Drift of a Device, on page 107](#).

Configuration drifts are captured when the following events occur:

- **First-Time Collection:** On adding a device to Cisco DNA Center, device configuration is collected.
- **Syslog-Based Collection:** Cisco DNA Center monitors syslog events sent by devices, and identifies the configuration changes. The configuration archive is triggered after 5 minutes, on occurrence of the latest event. Based on the login IP address in syslog events, configuration drifts are marked in-band (configuration changes done by Cisco DNA Center) or out-of-band (configuration changes done outside Cisco DNA Center).



Note New traps within the 5-minute window will restart the timer to avoid multiple archives with partial changes. For accurate results, we recommend that you wait for at least 5 minutes.

- **Weekly Backup Collection:** Cisco DNA Center performs periodic weekly backup of device configurations. When no events are received for a device, the configuration changes made outside or from Cisco DNA Center are captured by the weekly backup archive. For more information, see [Configure Device Configuration Backup Settings](#) in the *Cisco DNA Center Administrator Guide*.



Note Configuration drifts detected by weekly backup archive are classified as in-band (configuration changes done by Cisco DNA Center), even though it is possible that the configuration changes were done outside Cisco DNA Center.

Disk utilization is optimized by ignoring the collected archive when no changes are present. Disk space optimization is not applicable for the first-time collection.



Tip To create a new configuration archive for a device, the configuration archive service relies on syslog traps from the network device. If you plan to use your own syslog server, you must continue to use the Cisco DNA Center server as the syslog server (in addition to any other syslog servers that you want to use) so that the configuration archive receives the latest configuration from the device.

View Configuration Drift of a Device

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

Step 2 In the **Devices** table, click the device name, and more information about the device is displayed.

Step 3 Click **View Device Details**.

The device details are displayed in the window.

Step 4 In the left pane, click **Config Drift**.

The **Configuration Changes** window shows the number of configuration drifts saved, which includes labeled configs and config drift versions.

Step 5 Expand the **Change History** tab to view the following details:

- a) **Config drift date range:** Click the **Start Date** and **End date** to choose the date range for which you want to view the config drift. By default, the start and end dates are set to display the config drift for the last 15 days.
- b) **Config drift timeline graph:** Shows the config drift for the chosen date range. By default, the last 15 days of config drift are shown in the timeline graph.

The timeline graph shows the following details:

- **In-band Config Drift:** Configuration changes done by Cisco DNA Center are shown as a blue bubble in the timeline graph.
 - **Out-of-band Config Drift:** Configuration changes done outside Cisco DNA Center are shown as a purple bubble in the timeline graph.
 - **Labeled Config:** The config version labeled and archived in Cisco DNA Center is shown as an orange bubble in the timeline graph. For more information, see [Label Configuration Drift, on page 108](#).
- c) **Config Drift Version:** Click the down arrow to view all the available config drift versions.
 - d) **Running Config:** Click the config drifts on the timeline graph. The comparison is shown under the **Running Config** tab. The differences between the config versions are marked in different colors for better visibility.

Label Configuration Drift

You can label the config drift on the timeline graph for future reference.

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** Click the device name, and more information about the device is displayed.
- Step 3** Click **View Device Details**.
Device details are displayed in the window.
- Step 4** In the left pane, click **Config Drift**.
The **Configuration Changes** window is displayed.
- Step 5** Choose the config drift in timeline graph that you want to label. The timestamp of the chosen config drift is shown in the **Config Drift Version** below the timeline graph.
- Step 6** Click **Label Config** corresponding to the chosen config drift version.
- Step 7** In the **Label Configuration** window, enter a name for the config version. The prefix of label config is fixed as CCA_.
Note Do not use special characters for the config version name.
- Step 8** Click **Save**. The labeled config drift is shown in orange in the timeline graph.
If the number of labeled config version is greater than the chosen range, change the total number of config drifts to be saved. For more information on how to configure number of config drifts to be saved, see the "Configure Device Configuration Backup Settings" section in the [Cisco DNA Center Administrator Guide](#).
- Step 9** To remove the label, select the labeled config version and click **Remove label**.

Replace a Faulty Device

The Return Material Authorization (RMA) workflow lets you replace failed devices quickly. RMA provides a common workflow to replace routers, switches, and APs.

When using the RMA workflow with routers and switches, the software image, configuration, and license are restored from the failed device to the replacement device. For wireless APs, the replacement device is assigned to the same site, provisioned with primary wireless controller, RF profile, and AP group settings, and placed on the same floor map location in Cisco DNA Center as the failed AP. For Cisco Switch stacks (hardware stacking), you do not need to follow a separate procedure in Cisco DNA Center for member switch replacement, it is handled by the active switch. The member switch is replaced by the active switch by providing software image and configuration. Full stack replacement is handled by Cisco DNA Center.



Note You can also replace a faulty device using the Replace Device workflow. For more details, see [Replace Device Workflow, on page 729](#).

Before you begin

- The software image version of the faulty device must be imported in the image repository before marking the device for replacement.
- The faulty device must be in an unreachable state.
- If the replacement device onboards Cisco DNA Center through Plug and Play (PnP), the faulty device must be assigned to a user-defined site.
- The replacement device must not be in a provisioning state while triggering the RMA workflow.
- For switch stacks replacement, the number of stacks for faulty and replacement device should be same.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window displays the device information that is gathered during the discovery process.

- a) Select the faulty device that you want to replace.
- b) From the **Actions** drop-down list, choose **Inventory > Device Replacement > Mark Device for Replacement**.
- c) In the **Mark for Replacement** window, click **Mark**.

Note To achieve seamless replacement of fabric devices, a DHCP server is configured on the neighbor device. This is required to assign an IP address to the replacement device for onboarding the device to Cisco DNA Center through PnP. This DHCP server is removed after successful replacement of the faulty device.

The latest configuration changes from the faulty device are pushed to the replaced device during the RMA workflow.

- d) From the **Inventory** drop-down list, choose **Marked for Replacement**.

A list of devices marked for replacement is displayed.

e) (Optional) If you do not want to replace the device, select the device and choose **Actions > Unmark for Replacement**.

Step 2

(Optional) To replace the device, do the following:

- a) Select the device that you want to replace and choose **Actions > Replace Device**.
- b) In the **Choose Replacement Device** window, choose a replacement device from the **Unclaimed** tab or **Managed** tab.

The **Unclaimed** tab shows the devices that are onboarded through PnP. The **Managed** tab shows the devices that are onboarded through the Inventory or the discovery process.

- c) (Optional) If the replacement device is not yet onboarded, do the following:
 1. In the **Choose Replacement Device** window, click **Add Device**.
 2. In the **Add New Device** window, enter the **Serial Number** of the device and click **Add New Device**.

Or

1. In the **Choose Replacement Device** window, click **Sync with Smart Account**.
2. In the **Sync with Smart Account** window, click **Sync**.

- d) Click **Next**.
- e) In the **Schedule Replacement** window, choose whether you want to start the device replacement immediately (if yes, click **Now**) or schedule it for later.
- f) Click **Review** to view the chosen device type, faulty device details, and replacement device details.
- g) Click **Next** to view the details in the **Summary** window.

In the **Summary** window, review the configuration settings.

- h) To make changes, click **Edit**.
- i) Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** window.
- j) Click **Replace Status** to view the status of the RMA workflow progress, as follows:
 - Running readiness checks for device replacement.
 - Claim the (PnP) replacement device.
 - Distribute and activate the software image to the replacement device.
 - Deploy licenses.
 - Provision VLAN configurations.
 - Provision startup configurations.
 - Reload the replacement device.
 - Check for reachability of the replacement device.
 - Deploy SNMPv3 credentials to the replacement device.
 - Synchronize the replacement device.
 - Remove the faulty device from CSSM.
 - Add the replacement device to CSSM.
 - Revoke and create the PKI certificate.

- Update Cisco ISE.
- Delete the faulty device.

After the workflow is complete, the **Replace Status** is updated to **Replaced**.

- k) If an error message appears, click the error link.
- l) Click **Retry** to retrigger the workflow with the same set of faulty and replacement devices.

The main inventory window displays the details of the new replacement device.

Note Marking the device for replacement and replacing the device can be done at different times.

Replace a Faulty Access Point

Using the AP RMA feature, you can replace a faulty AP with a replacement AP available in the device inventory.

Before you begin

- The AP Return Material Authorization (RMA) feature supports only like-to-like replacement. The replacement AP must have the same model number and PID as the faulty AP.
- The replacement AP must have joined the same Cisco Wireless Controller as the faulty AP.
- A Cisco Mobility Express AP that acts as the wireless controller is not a candidate for the replacement AP.
- The software image version of the faulty AP must be imported in the image repository before marking the device for replacement.
- The faulty device must be assigned to a user-defined site if the replacement device onboards Cisco DNA Center through Plug and Play (PnP).
- The replacement AP must not be in provisioning state while triggering the RMA workflow.
- The faulty device must be in an unreachable state.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The **Inventory** window displays the device information that is gathered during the discovery process.
 - Step 2** Check the check box of the faulty AP that you want to replace.
 - Step 3** From the **Actions** drop-down list, choose **Device Replacement > Mark Device for Replacement**.
 - Step 4** In the **Mark for Replacement** window, click the radio button next to the faulty device name.
 - Step 5** From the **Actions** drop-down list, choose **Replace Device**.
 - Step 6** In the **Replace Device** window, click **Start**.
 - Step 7** In the **Available Replacement Devices** table, click the radio button next to the replacement device name.
 - Step 8** Click **Next**.

- Step 9** Review the **Replacement Summary** and then click **Next**.
- Step 10** In the **Schedule Replacement** window, select whether to replace the device now, or schedule the replacement for a later time, and then click **Submit**.
The RMA workflow begins.
- Step 11** To monitor the replacement status, under **What's Next**, click **Monitor Replacement Status**.
The **Mark For Replacement** window lists the devices that are marked for replacement.
Check the status of the replacement in the **Replace Status** column, which initially shows **In-Progress**.
- Step 12** Click **In-Progress** in the **Replace Status** column.
The **Replace Status** tab shows the various steps that Cisco DNA Center performs as part of the device replacement.
- Step 13** In the **Marked for Replacement** window, click **Refresh** and click **Replace Status** to view the replacement status.
If the faulty AP replacement fails, then the **Replace Status** column shows the reason for failure with an error message.
You can either replace the faulty AP with another new AP or retry the failed replacement using the AP RMA Retry feature.
- Step 14** To retry the failed replacement, click the error message in the **Replace Status** column against the device name.
- Step 15** Click **Retry**.
- Step 16** In the **Marked for Replacement** window, click **In-Progress** against the **Replace Status** column.
The **Replace Status** tab shows success after successful replacement of the faulty AP.
- Step 17** The **Replace Status** in the **Replacement History** window shows **Replaced** after the faulty device is replaced successfully.
- Step 18** (Optional) If you do not want to replace the device, select the device and choose **Actions > Unmark for Replacement**.
-

Limitations of the RMA Workflow in Cisco DNA Center

- RMA supports replacement of similar devices only. For example, a Cisco Catalyst 3650 switch can be replaced only with another Cisco Catalyst 3650 switch. Also, the platform IDs of the faulty and replacement devices must be the same.
- RMA supports replacement of all switches, routers, and Cisco SD-Access devices, *except for the following*:
 - Devices with embedded wireless controllers
 - Cisco Wireless Controllers
 - Chassis-based Nexus 7700 Series Switches
 - Switch stacks (SVL stacking)
- RMA supports devices with an external SCEP broker PKI certificate. The PKI certificate is created and authenticated for the replacement device during the RMA workflow. The PKI certificate of the replaced faulty device must be manually deleted from the certificate server.
- The RMA workflow supports device replacement only if:
 - Both the faulty and replacement devices have the same extension cards.

- The number of ports in both devices does not vary because of the extension cards.
- The faulty device is managed by Cisco DNA Center with a static IP. (RMA is not supported for devices that are managed by Cisco DNA Center with a DHCP IP, except extended node and AP in fabric.)
- Fabric edge replacement does not support the DHCP server configuration in the neighbor device if the neighbor device is not part of the fabric. Because intermediate nodes are not part of the Cisco SD-Access fabric, the DHCP server with option 43 is not pushed.
- Make sure that the replacement device is connected to the same port to which the faulty device was connected.
- Cisco DNA Center does not support legacy license deployment.

The RMA workflow deregisters the faulty device from Cisco SSM and registers the replacement device with Cisco SSM.

- If the software image installed on the faulty device is earlier than Cisco IOS XE 16.8, the **License Details** window does not display the Network and Feature License details and no warning message is displayed. Therefore, you should be aware of the legacy network license configured on the faulty device and manually apply the same legacy network license on the replacement device.
- If the software image installed on the faulty device is Cisco IOS XE 16.8 or later, the **License Details** window displays details of the network license (for example, **Legacy** or **Network**) and the feature license (for example, IP Base, IP Service, or LAN Base). The following warning message is displayed while marking the faulty device for replacement:

```
Some of the faulty devices don't have a Cisco DNA license. Please ensure your replacement device has the same Legacy license of the faulty device enabled.
```

- If the legacy network licenses of the replacement and faulty devices do not match, the following error message is displayed during the license deployment:

```
Cisco DNA Center doesn't support legacy license deployment. So manually update the faulty device license on the replacement device and resync before proceeding.
```

- Cisco DNA Center supports PnP onboarding of the replacement device in a fabric network, *except when*:
 - The faulty device is connected to an uplink device using multiple interfaces.
 - LAN automation uses overlapping pools.
- If the replacement device onboards through the PnP-DHCP functionality, make sure that the device gets the same IP address after every reload and the lease timeout of DHCP is longer than two hours.

Reboot Access Point

Using the AP Reboot feature, you can reboot one or more APs for troubleshooting and maintenance.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

Step 2 Check the check box of the APs that you want to reboot.

Step 3 From the **Actions** drop-down list, choose **Inventory > Reboot Device**.

Step 4 In the **Reboot Device** slide-in pane, choose whether you want to reboot the AP **Now** or schedule it for later.

Step 5 Expand **Selected Devices** to view the AP name and floor details of the reboot AP.

Step 6 Click **Reboot**.

After the Cisco Wireless Controller initiates the task of rebooting the selected APs, a message saying *Reboot Initiated Successfully* is displayed.

Step 7 In the **Task Submitted** dialog box, click the **Task** link.

This dialog box displays for a few seconds and then disappears. To navigate to the task, click the menu icon (☰) and choose **Activities > Tasks**.

Step 8 Click the task name to view the reboot initiation status.



CHAPTER 6

Display Your Network Topology

- [About Topology, on page 115](#)
- [Display the Topology of Areas, Sites, Buildings, and Floors, on page 116](#)
- [Filter Devices on the Topology Map, on page 116](#)
- [Display Device Information, on page 117](#)
- [Display Link Information, on page 118](#)
- [Pin Devices to the Topology Map, on page 119](#)
- [Assign Devices to Sites, on page 119](#)
- [Save a Topology Map Layout, on page 119](#)
- [Open a Topology Map Layout, on page 120](#)
- [Share a Topology Map Layout, on page 120](#)
- [Export the Topology Layout, on page 121](#)

About Topology

The **Topology** window displays a graphical view of your network. Using the Discovery settings that you have configured, Cisco DNA Center discovers the devices in your network and assigns a device role to them. Based on the device role assigned during discovery (or changed in Device Inventory), Cisco DNA Center creates a physical topology map with detailed device-level data.

Using the topology map, you can do the following:

- Display the topology of a selected area, site, building, or floor.
- Display detailed device information.
- Display detailed link information.
- Filter devices based on a specific Layer 2 VLAN.
- Filter devices based on a Layer 3 protocol (such as Intermediate System - Intermediate System [IS-IS], Open Shortest Path First [OSPF], Enhanced Interior Gateway Routing Protocol [EIGRP], or static routing).
- Filter devices with Virtual Routing and Forwarding (VRF) capability.
- Pin devices to the topology map.
- Save a topology map layout.
- Open a topology map layout.

- Export screen shots of the complete topology layout in PNG format.

Display the Topology of Areas, Sites, Buildings, and Floors

You can display the topology of an area, site, building, or floor.

Before you begin

- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.
- You must have defined a network hierarchy and provisioned devices to the buildings or floors within it.

Step 1 Click the menu icon () and choose **Tools > Topology**.

Step 2 In the left tree view menu, select the area, site, building, or floor that you are interested in.




Step 3 Use the Toggle button to switch between the Geographical map view and the Layer 2 map view.

The Geographical map view displays the sites. The nearer sites are grouped together and indicated with the number of sites in the group. The device health is indicated in different colors. Hover over the site to view the detailed device health.

Use the Search field in the top right corner to find a building in the Geographical map view, and a device in the Layer 2 map view.

Note

- Click the  icon in the lower-right corner to open a legend that shows the available shortcut keys for the topology maps.
- Click the **Toggle Annotate** icon to draw annotations in the Layer 2 map. You can click the export icon to export the topology map along with the annotations.

Step 4 Click **Take a Tour** to know the details of various options available in the **Topology** window.

Filter Devices on the Topology Map

You can filter devices based on one of the following attributes:

- VLAN
- Routing
- VRF
- Tagging

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Tools > Topology**.

Step 2 Click **Filter**.

Note If you are not able to view the **Filter**, click a site in the left tree view menu.

Step 3 Do one of the following:

- From the **VLAN** drop-down list, choose the VLAN that you want to view.
- From the **Routing** drop-down list, choose the protocol that interests you.
- From the **VRF** drop-down list, choose the VRF that you want to view.
- Click **View All Tags** and choose the tags you want to view. The devices associated with the selected tags will be highlighted. If you want to create a new tag, do the following:

- a) Click **Create New Tag**.
- b) Enter the **Tag Name**.
- c) Click **Save**.

You can also associate a device with the tag by doing the following:

- a) Click the device.
 - b) Click **Tag Device**.
 - c) Select the tag to which you want to associate the device.
 - d) Click **Apply**.
-

Display Device Information

Cisco DNA Center allows you to display the device name, IP address, and software version of devices.



Note The device information that is accessible in the **Topology** window is also accessible in the **Device Inventory** window.

Before you begin


Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Tools > Topology**.

Step 2 In the tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 In the topology area, hover your mouse over the device or device group that interests you.

Note A device group is labeled with the number and types of devices it contains. A blue arrow under a switch indicates that switch has a host. Click the blue arrow to view the host.

Step 4 Click **Display** and enable the following items to view additional device details. For more information, hover your mouse over the  icon next to the items.

- **Device Health:** Displays the health of the devices.
- **Link Health:** Displays the health of the links between the devices.
- **License status:** Displays the license status of the device. Cisco DNA Center highlights a device if its license is about to expire and a warning icon appear next to it. Click the highlighted device to view its license details.
- **Device IP:** Displays device IP address under device label.
- **Device Suffixes:** Displays full name of the device, with its suffix.

Note Topology uses Link Layer Discovery Protocol (LLDP) to determine the neighbor devices when network devices are not configured with Cisco Discovery Protocol (CDP) in Cisco DNA Center.

Display Link Information

Cisco DNA Center allows you to display information about the links in the topology map. For simple links, the display shows information for the single link. For aggregated links, the display shows a listing of all the underlying links. The information includes the interface name, its speed, and its IP address.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon () and choose **Tools > Topology**.

Step 2 In the tree view menu, select the area, site, building, or floor that you are interested in.

Step 3 Hover your cursor over the link that interests you.

Step 4 Click **Display** and enable **Link Health**.

A down link is shown in red. If you want to delete the link, select it and click **Delete**. You can bring the link up by doing the following:

- a) Log in to the device.
- b) Enable the interface.
- c) Resynchronize the device on the Inventory page.

Note Topology uses Link Layer Discovery Protocol (LLDP) to determine the links for devices that are discovered using LLDP in Cisco DNA Center.

Pin Devices to the Topology Map

Devices can be grouped or aggregated so that they take up less room on the map. However, at times, you might want to separate a device from its group. You can do this by pinning a device to the map.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Tools > Topology**.

Step 2 Do one of the following:

- To pin a device, click the device group, and in the dialog box, click the pin icon to the left of the device name.
- To pin all the devices, click the device group, and, in the dialog box, click **Pin All**.

Note Double click the group to unpin the devices in the group.

Assign Devices to Sites

Devices can be assigned to specific sites using the topology map.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Tools > Topology**.

Step 2 Click **Unassigned Devices** in the left pane. All the unassigned devices are displayed in the topology area.

Step 3 Click the device for which you want to assign a site. Device details are displayed in a pop-up window. In the **Assign devices to:** section, click the **choose the location** drop-down list to select a location.

Step 4 (Optional) To assign the site only for the selected device and not for the connected (downstream) devices, uncheck the **Auto-assign unclaimed downstream devices** check box.


Step 5 Click **Assign**.

Save a Topology Map Layout

Cisco DNA Center has a Cisco-recommended topology layout that is displayed by default when you open the topology tool. You can customize multiple layouts and save them to view later. You can also set one of the layouts as the default to be displayed when you open the topology map.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.


- Step 1** Click the menu icon () and choose **Tools > Topology**.
 - Step 2** Click **Custom View**.
 - Step 3** In the **Enter View Title** field, enter a name for your customized map.
 - Step 4** Click **Save**.
 - Step 5** (Optional) To set your customized map as the default, click **Make Default**.
-

Open a Topology Map Layout

You can open previously saved topology maps.

Before you begin

You should have saved topology map layouts.


- Step 1** Click the menu icon () and choose **Tools > Topology**.
 - Step 2** Click **Custom View**.
 - Step 3** Click the name of the map that you want to display.
-

Share a Topology Map Layout

You can share a customized map with other users.

Before you begin

- You must have topology map layouts saved.
 - You must have at least one topology view saved.
-

- Step 1** Click the menu icon () and choose **Tools > Topology**.
 - Step 2** Click **Custom View**.
 - Step 3** Hover the cursor over the name of the custom map and click the **Share Focus** icon.
 - Step 4** In the confirmation window, click **Yes**.
-


Export the Topology Layout

You can export a snapshot of the full topology layout. The snapshot is downloaded as a SVG, PDF, PNG file to your local machine.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 Click the menu icon (☰) and choose **Tools > Topology**.

Step 2 Click  (this icon represents **Export Topology**).

Step 3 Select a file format and click **Export**.



PART **III**

Design Your Network

- [Design the Network Hierarchy, on page 125](#)
- [Work with Wireless 2D and 3D Floor Maps, on page 139](#)
- [Configure Network Settings, on page 191](#)
- [Configure Network Profiles, on page 275](#)



CHAPTER 7

Design the Network Hierarchy




- [Network Hierarchy Overview, on page 125](#)
- [Design a New Network Hierarchy, on page 126](#)
- [Use an Existing Cisco Network Hierarchy, on page 126](#)
- [Use an Existing Ekahau Network Hierarchy, on page 129](#)
- [Export Your Network Hierarchy from Cisco DNA Center, on page 132](#)
- [Search the Network Hierarchy, on page 134](#)
- [Create a New Network Hierarchy, on page 134](#)

Network Hierarchy Overview

You can create a network hierarchy that represents your network's geographical locations. The hierarchical organization enables you to easily apply design settings or configurations to a specific hierarchical element. For example, you can apply design settings to an entire area or to only a floor.

You can name hierarchical elements to help you identify where to apply design settings later.

The hierarchical elements that you can create have rules that dictate under which elements they can reside and which elements can reside under them.

- **Global**: Default element under which all other hierarchical elements reside. Areas and sites are the only elements that can reside directly under **Global**.
- **Areas** and **Sites** (): Areas and sites reside under **Global** or under other areas or sites. They do not have a physical address. As the largest element, they identify a geographic region. They provide a way to group areas and sites.
- **Buildings** (): Buildings reside under areas or sites. When you create a building, specify a physical address or latitude and longitude coordinates. Buildings can't contain areas. However, they can contain floors.
- **Floors** (): Floors reside under buildings. You can add floors to buildings with or without maps that contain various building components, like walls and windows. If you decide to use floor maps, you can manually create them or import them from files, such as DXF, DWG, JPG, GIF, PNG, or PDF file types. Then you can position your wireless devices on the floor maps to visualize your wireless network coverage.

You can change the site hierarchy for unprovisioned devices while preserving AP locations on floor maps. Note, however, that you can't move an existing floor to a different building.

To get started, build your network hierarchy using one of the following methods:

- Create a new network hierarchy. For more information, see [Create a New Network Hierarchy, on page 134](#).
- Import an existing network hierarchy from Cisco Prime Infrastructure or Ekahau Pro. For more information, see [Use an Existing Cisco Network Hierarchy, on page 126](#) or [Use an Existing Ekahau Network Hierarchy, on page 129](#).

Design a New Network Hierarchy

The **Design** area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the **Design** workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the **Discovery** feature. For more information, see [Discovery Overview, on page 37](#).

You can perform these tasks in the **Design** area:

-
- Step 1** Create your network hierarchy. For more information, see [Create, Edit and Delete a Site, on page 134](#).
 - Step 2** Define global network settings. For more information, see [Network Settings Overview, on page 191](#).
 - Step 3** Define network profiles. For more information, see [Network Profiles Overview, on page 275](#).
-

Use an Existing Cisco Network Hierarchy

If you have an existing network hierarchy in Cisco Prime Infrastructure, you can export it and then import it into Cisco DNA Center, saving time and effort spent in creating a new network hierarchy.

The following information is available for you to re-create your network hierarchy:

- **Site Hierarchy:** Your existing site hierarchy is downloaded in a CSV file format. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.
- **Map Archive:** Map information is downloaded as a map archive in a TAR file format. The map archive file contains data such as the date and time, number of floors, and APs. Depending on what you choose to download, the map archive can also include map information, such as floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps. You can also choose to download calibration information, such as the RF attenuation model that has been applied to each floor.

You can choose to base the map archive on the global hierarchy or the hierarchy of a single site, building, or floor, as follows:

- **Site:** The chosen site and all of its subsites, buildings, and floors are exported.
- **Building:** The chosen building and all of its floors are exported.
- **Floor:** The chosen floor is exported.



Note Cisco DNA Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Cisco DNA Center image. By default, FIPS mode is disabled.

FIPS mode has the following impact on the export and import of map archives.

If FIPS mode is *enabled*:

- Exported map archives are unencrypted.
- Only unencrypted map archives can be imported.

If FIPS mode is *disabled*:

- Exported map archives are encrypted.
- Both encrypted and unencrypted map archives can be imported.

Export Your Site Hierarchy from Cisco Prime Infrastructure

You can export your site hierarchy from Cisco Prime Infrastructure in a CSV file format. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

Before you begin

Site hierarchy export is supported in Cisco Prime Infrastructure, Release 3.2 and later.

-
- Step 1** In Cisco Prime Infrastructure, choose **Inventory > Group Management > Network Device Groups**.
- Step 2** In the **Device Groups** window, click **Export Groups**.
- Step 3** In the **Export Groups** dialog box, click the **APIC-EM** radio button.
- Step 4** To download the CSV file, click **OK**.
The CSV file is downloaded.
-

Export Your Map Archive from Cisco Prime Infrastructure

You can export map archive files from Cisco Prime Infrastructure and import them into Cisco DNA Center. Map archives contain map information, such as floor dimensions, and calibration information, such as the Radio Frequency (RF) attenuation model that has been applied to each floor in Cisco Prime Infrastructure.

-
- Step 1** From the Cisco Prime Infrastructure GUI, choose **Maps > Wireless Maps > Site Maps (New)**.
- Step 2** From the **Export** drop-down list, choose **Map Archive**.
The **Export Map Archive** window opens, and the **Select Sites** window opens by default.

Step 3 Check the check box adjacent to a specific site, campus, building, or floor that you want to export. Alternatively, check the **Select All** check box to export all the maps.

Step 4 Select at least one of the following options:

- **Map Information:** Click the **On** button to export floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps.
- **Calibration Information:** Click the **On** button to export the RF attenuation model that has been applied to each floor. It is a good practice to export the existing calibration data from Cisco Prime Infrastructure. Otherwise, you must re-enter the calibration details manually.

If you choose to include calibration information, you also need to specify whether to include information for the selected maps or all the information, as follows:

- **Calibration Information for selected maps:** Calibration information for the selected site maps is exported.
- **All Calibration Information:** Calibration information for the selected map and any additional calibration information that is available in the system is exported.

Step 5 Click **Generate Map Archive**.

The following message shows the progress of the operation:

```
Exporting data is in progress
```

A TAR file is created and is saved to your local machine.

Step 6 Click **Done**.

Import Your Site Hierarchy to Cisco DNA Center

You can import a site hierarchy that you exported from Cisco Prime Infrastructure as a CSV file. For information about exporting the site hierarchy, see [Export Your Site Hierarchy from Cisco Prime Infrastructure, on page 127](#).

Before you begin

- Make sure that you have Cisco Wireless Controllers and APs in your Cisco DNA Center inventory. If not, discover them using the **Discovery** feature.
 - Add and position APs on a floor map.
 - If you manually created sites in Cisco DNA Center that are present in Cisco Prime Infrastructure, you must remove them from Cisco DNA Center before you can import them.
-

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the map tool bar, click **Import** and choose **Import Sites**.

Step 3 In the dialog box, click one of the following radio buttons:

- **Merge with Existing Sites:** The downloaded site information is combined with the existing site information.

- **Overwrite Existing Sites:** If the same site already exists in Cisco DNA Center, the existing site information is overwritten with the downloaded site information.

Step 4 In the dialog box, drag and drop your CSV file into the download area. Alternatively, you can click **Choose a file** and navigate to where your CSV file is located, then click **Upload**.

Note If you do not have a CSV file, click **Download Template** to download a CSV file that you can edit and upload.

Import Your Map Archive to Cisco DNA Center

You can import a map archive TAR file into Cisco DNA Center. For example, you can upload the TAR file that you exported from Cisco Prime Infrastructure.



Note Cisco DNA Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Cisco DNA Center image. By default, FIPS mode is disabled.

For information about exporting site hierarchy, see [Export Your Map Archive from Cisco Prime Infrastructure, on page 127](#).

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the map toolbar, click **Import** and choose **Import Maps**.

Step 3 In the **Import Maps** dialog box, drag and drop the map archive file.

Step 4 Click **Import**.

The map archive file is imported.

Use an Existing Ekahau Network Hierarchy

The Ekahau Pro tool allows you to create a complete network plan for your enterprise, including floor layout, AP locations, and obstacles. After creating the floor layout, you can export the simulated network plan as an Ekahau project file. You can also export the real-world site survey data into a format that Cisco DNA Center can use.

Export an Ekahau Project

You can export your network hierarchy from Ekahau Pro and import it into Cisco DNA Center for further planning.

Step 1 In the Ekahau Pro tool, plan the floor layout:

- Create buildings and floors.

It is not mandatory to create buildings in the Ekahau Pro tool.

- Import the floor plan.
- Add the planned APs or hypothetical APs.
- Add building coordinates.
- Define the site name.

The AP name that you provide here will be used to update the AP name on the Cisco Wireless Controller during the wireless controller configuration.

- Add obstacles.
- Export the project.

Note If you're using Ekahau Cloud, make sure to synchronize any local changes to the Ekahau Cloud before exporting the Ekahau project. If the Ekahau project has local changes (such as the removal of an AP or wall) that are out-of-sync with the Ekahau Cloud project, importing the Ekahau project to Cisco DNA Center can fail.

Step 2 Deploy the planned APs at locations designed on the floor layout.

- The physical AP is mounted at the designed location that is specified on the floor layout. The MAC address of the planned AP is updated with the MAC address of the physical AP.
- The physical AP is connected to the VLAN of the intended wireless controller.

Step 3 In Cisco DNA Center, configure the Cisco Wireless Controller.

- a. Discover the Cisco Wireless Controller and APs in your network by running the **Discovery** job, so that the discovered wireless controllers and APs are listed on the **Inventory** window.
- b. Update the AP name on the wireless controller with the AP name given in the Ekahau Pro project during the floor planning.

Step 4 Import the Ekahau project into Cisco DNA Center.

Step 5 Map the planned APs to real APs in Cisco DNA Center.

Import an Ekahau Project to Cisco DNA Center

Before you begin

Importing an Ekahau Cloud project can fail if the project has local changes (such as removing an AP or wall), that are out-of-sync with the Ekahau Cloud project. To avoid this situation, make sure to synchronize any local changes to the Ekahau Cloud before importing the Ekahau Cloud project to Cisco DNA Center.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** Design your network hierarchy by adding sites, buildings, and floors.
- Note** For more information, see [Create, Edit and Delete a Site, on page 134](#), [Add, Edit, and Delete a Building, on page 135](#), and [Add, Edit, and Delete a Floor, on page 136](#).
- While adding floors, make sure that you create floors with the same name given in the Ekahau project.
- Step 3** In the left pane, hover your cursor over the ellipsis ●●● icon next to the site where you want to import the Ekahau project and choose **Import Ekahau Project**.
- The **Import Ekahau Project** dialog box appears.
- Step 4** Drag and drop the ESX file into the boxed area in the **Import Ekahau Project** dialog box, or click the **click to select** link and browse to the ESX file.
- Note** To import buildings, they need to contain coordinates inside the Ekahau Project. You can add coordinates in Ekahau Pro. After successfully importing an Ekahau Project, each planned AP is mapped to an existing real AP in the inventory using the AP name. The planned AP is displayed with an icon **P** on the floor map. For example, if the name of the planned AP is SJC01-02-AP-B-1, the import process searches for the real AP with the same name.
- Step 5** If an AP is not found in the inventory and remains unmapped, the planned AP is retained on the floor.
- To see the reason for the mismatch, hover your cursor over the planned AP icon on the floor map, and click **Import History**.
- The following attempts are made to map the planned APs to real APs:
- If the newly discovered APs match the planned AP, the planned AP is replaced with the discovered real AP.
 - If a planned AP remains unmapped, you can manually replace the planned AP with the real AP, providing reasons for the failure.
- Step 6** To manually assign the planned AP to a real AP, hover your cursor over the planned AP icon on the floor map, and click **Assign > Assign**.
- The **Assign Planned APs** panel appears.
- Step 7** In the **Assign Planned APs** panel, map the planned AP to a real AP by AP name, AP type, or All APs.
- Step 8** Click the radio button next to the AP Name, and click **Assign** to manually assign the planned AP.
- Step 9** Click **Save**.
-

Import an Ekahau Site Survey to Cisco DNA Center

You can upload an Ekahau site survey to create the buildings and floors in your network hierarchy. The site survey includes information about wireless devices, including the site, building, and floor to which it is assigned and its position on the floor map. However, it doesn't include the AP antenna information. So, you need to upload this information separately using a CSV file.

Cisco DNA Center includes a CSV template file that you can download and edit to define the required AP antenna information.

Figure 3: The CSV template file contains the following fields and defaults:

	A	B	C	D	E	F	G	H	I	J
1	model	antennaName0	antennaAzimuth0	antennaElevation0	antennaName1	antennaAzimuth1	antennaElevation1	antennaName2	antennaAzimuth2	antennaElevation2
2	AP2700I	Internal-2700-5GHz	90d	0d	Internal-2700-2.4GHz	90d	0d			
3	AP1850I	Internal-1850-5GHz	90d	0d	Internal-1850-2.4GHz	90d	0d			
4	AP3800E	AIR-ANT2524DB-R-5GHz	179.9543762d	0d	AIR-ANT2524DB-R-2.4GHz	179.9543762d	0d			
5										

If an AP isn't in the Cisco DNA Center device inventory, it's imported as a planned AP. However, you can use a naming convention so that when you add an AP to the device inventory, Cisco DNA Center can automatically convert it to an actual AP.

The naming convention is AP, followed by the last four digits of the AP's MAC address, for example, AP-c4:e0. Using this information, Cisco DNA Center attempts to match the provided digits with the last four digits of an AP's Ethernet MAC or radio MAC address. If this information isn't available or a match is unsuccessful, Cisco DNA Center attempts to match AP names.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 Click **Add Site > Add Area**.

Alternatively, you can hover your cursor over the ellipsis ... next to the parent site or **Global** in the left pane, and choose **Add Area**. For more information, see [Create, Edit and Delete a Site, on page 134](#).

Step 3 In the left pane, hover your cursor over the ellipsis ... icon next to the site you just created and choose **Import Ekahau Survey**.

Step 4 In the **Import Ekahau Survey** dialog box, drag and drop the Ekahau Survey file into the **Ekahau Survey** boxed area, or click the **Choose a file** link and browse to the ESX file.

Step 5 Drag and drop the CSV file into the **AP Mapping CSV** boxed area, or click the **Choose a file** link and browse to the CSV file.

Note If you do not have a CSV file, click **Download AP Mapping Template** to download a CSV file that you can edit and upload.

Step 6 Click **Import**.

After the files are successfully downloaded, a success message is displayed.

Step 7 Click **View Hierarchy** and navigate to the floors to verify that the devices have been imported and positioned properly.

Hover the cursor over a device to view its details.

Export Your Network Hierarchy from Cisco DNA Center

You can export a site hierarchy to a CSV format file. You can also export a complete network map (global hierarchy) or the hierarchy of a site, building, or floor. You can choose either a Cisco Prime Infrastructure or Ekahau Pro format. Exporting your network hierarchy into these formats allows you to continue to work on your network hierarchy in these tools.

Export Your Site Hierarchy from Cisco DNA Center

You can export a site hierarchy to a CSV format file. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the map toolbar, click **Export** and choose **Export Sites**.
- Step 3** In the **Export Sites** dialog box, click **OK**.
-

Export Your Map Archive from Cisco DNA Center

You can export a complete network map (global hierarchy) or the hierarchy of a site, building, or floor to either a Cisco Prime Infrastructure or Ekahau Pro format. You can export up to 500 floors.



Note Cisco DNA Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Cisco DNA Center image. By default, FIPS mode is disabled.

FIPS mode has the following impact on the export and import of map archives.

If FIPS mode is *enabled*:

- Exported map archives are unencrypted.
- Only unencrypted map archives can be imported.

If FIPS mode is *disabled*:

- Exported map archives are encrypted.
 - Both encrypted and unencrypted map archives can be imported.
-

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** To export the complete network map, from the map toolbar, click **Export** and choose **Export Maps**.
Alternatively, from the left pane, hover your cursor over the ellipsis (⋯) next to a site, building, or floor and choose **Export Maps**.

The information that is exported depends on what you choose:

- **Site**: The chosen site and all of its subsites, buildings, and floors are exported.
- **Building**: The chosen building and all of its floors are exported.
- **Floor**: The chosen floor is exported.

- Step 3** In the **Export Maps** dialog box, click either the **Ekahau Project** or the **Prime** radio button.

Step 4 Click **Export**.

Search the Network Hierarchy

You can search the network hierarchy to quickly find a site, building, or area. This is particularly helpful after you have added many sites, areas, or buildings.

Step 1 To search the hierarchy, from the **Search Hierarchy** search field in the left pane, enter either the partial or full name of the site, building, or floor name that you are searching.

The hierarchy is filtered based on the text you enter in the search field.

Step 2 To search the hierarchy by **Site Name** and **Site Type** filter criteria, click the filter icon in the **Search Hierarchy** search field and do the following:

- a. In the **Site Name** field, enter the name of the site that you want to search.
- b. Check the **Include Address for all Building** check box to include the address of all building in the search result.
- c. In the **Site Type** area, check the check boxes next to **Area**, **Building**, or **Floor** that you want to include in filter criteria.
- d. Click **Search**.

The hierarchy is filtered based on the filter criteria.

- e. To exclude the search criteria in the left pane, click the cross-mark next to respective criteria.
-

Create a New Network Hierarchy

Create a new network hierarchy by creating new sites (or areas), building, and floors.

Create, Edit and Delete a Site

Cisco DNA Center allows you to easily define physical sites and then specify common resources for those sites. The **Design** area uses a hierarchical format for intuitive use, while eliminating the need to redefine the same resource in multiple places when provisioning devices. By default, there is one site called **Global**. You can add more sites, buildings, and areas to your network hierarchy. You must create at least one site before you can use the provision features.

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

A world map appears in the right pane.

Step 2 From this window, you can add, edit, and delete sites. See the following table for details.

Action	Steps
Add a site.	<p>a. From the map toolbar, click + Add Site > Add Area.</p> <p>Alternatively, you can hover your cursor over the ellipsis ... next to the parent site in the left pane, and choose Add Area.</p> <p>b. In the Area Name field, enter the site name.</p> <p>The Area Name field has the following restrictions:</p> <ul style="list-style-type: none"> • The area name cannot exceed 40 characters. • Special characters & > < ? ' " / [] aren't allowed. <p>c. From the Parent drop-down list, choose a parent node. Global is the default parent node.</p> <p>d. Click Add.</p>
Edit a site.	<p>a. In the left pane, hover your cursor over the ellipsis ... next to the site and choose Edit Area.</p> <p>b. In the Edit Area dialog box, make the necessary edits.</p> <p>c. Click Update.</p>
Delete a site.	<p>a. In the left pane, hover your cursor over the ellipsis ... next to the site and choose Delete Area.</p> <p>b. Click OK.</p>

Add, Edit, and Delete a Building

Step 1 Click the menu icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2 From this window, you can add, edit, and delete a building. See the following table for details.

Action	Steps
Add a building.	<p>a. In the Network Hierarchy window, click +Add Site > Add Building.</p> <p>Alternatively, you can hover your cursor over the ellipsis ... next to the parent site in the left pane, and choose Add Building.</p> <p>b. In the Add Building dialog box, add the building details.</p> <p>The Building Name field has the following restrictions:</p> <ul style="list-style-type: none"> • The building name cannot exceed 40 characters. • Special characters & < ? ' " / [] aren't allowed. <p>You can enter the address in the field or click the map. Adding an address causes the Longitude and Latitude coordinate fields to be automatically populated. These coordinates correspond to the northwest corner of the building and are used by location services, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), if they are integrated with Cisco DNA Center.</p> <p>c. Click Add.</p>
Edit a building.	<p>a. In the left pane, hover your cursor over the ellipsis ... next to the site and choose Edit Building.</p> <p>b. In the Edit Building dialog box, make the necessary edits.</p> <p>c. Click Update.</p>
Delete a building.	<p>a. In the left pane, hover your cursor over the ellipsis ... next to the building and choose Delete Building.</p> <p>b. Click OK.</p>


Add, Edit, and Delete a Floor

After you add a building, you can add floors to it. You can add a basic floor that doesn't have a floor map and add the floor map later, or you can add a floor and include a floor map at the same time.

To add a basic floor to a building, use this procedure.

To add a floor and a floor map at the same time, see one of the following topics:

- [Add a Floor with a CAD Map File, on page 141](#)
- [Add a Floor with a Non-CAD Map File, on page 142](#)
- [Import an Ekahau Project to Cisco DNA Center, on page 130](#)

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

Step 2 From this window, you can add, edit, and delete a floor. See the following table for details.

Action	Steps
Add a basic floor	<ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the desired building and choose Add Floor. b. In the Floor Name field, enter a name for the floor. The Floor Name field has the following restrictions: <ul style="list-style-type: none"> • The floor name cannot exceed 40 characters. • Special characters & > < ? ' " / [] aren't allowed. c. If you have wireless devices, for the Type (RF Model) drop-down list, choose the RF model to apply to the floor. The RF model determines how the RF is calculated when computing 2D and 3D heatmaps that show the relative intensity of the RF signals in the coverage area. d. Configure the Floor Number, Floor Type and Floor Thickness fields. The floor type and thickness are used when calculating a heatmap for wireless devices. e. Skip uploading a floor map image in Floor Image area. f. Configure map dimensions in the Width, Length, and Height fields. g. Click Add.
Edit a floor	<ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the floor and choose Edit Floor. b. In the Edit Floor dialog box, make the necessary changes. c. Click Update to save the changes.
Delete a floor	<ol style="list-style-type: none"> a. In the left pane, hover your cursor over the ellipsis ... next to the floor and choose Delete Floor. b. Click Ok.



CHAPTER 8

Work with Wireless 2D and 3D Floor Maps

- [Work with Floor Maps, on page 139](#)
- [Add a Floor with a Map File, on page 140](#)
- [Work with 2D Maps, on page 145](#)
- [Work with 3D Maps, on page 172](#)

Work with Floor Maps

There are several reasons to add floors with floor maps. One reason is to see your wireless network the way it exists today. Another reason is to help you plan and visualize future changes.

You can visualize your wireless network by creating or importing a floor map that contains various building components, like walls and windows, and then positioning your wireless devices on it. Using the floorplan, Cisco DNA Center computes 2D and 3D heatmaps that show the relative intensity of the RF signals in the coverage area. For 2D wireless maps, the heatmap is only an approximation of the actual RF signal intensity because it does not consider the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions. In either case, we recommend that you import a file with an existing floor plan to get started.

Interactive planning helps you plan a floor layout by drawing planned, or hypothetical, APs and obstacles with a raster image or a CAD floor plan as the backdrop. You can export the floor map as a PDF and share it with the technicians who are mounting the APs. The floor drawing helps the technicians to visualize the floor layout and the exact AP mount locations.

With interactive floor planning, you can:

- Create a floor layout with a raster or CAD floor plan as the canvas.
- Place the planned APs or hypothetical APs on the floor map based on the signal coverage requirement. These hypothetical APs or planned APs are not yet installed or discovered by Cisco DNA Center.
- Assign the antenna type and orientation.
- Draw obstacles, such as walls and shelving on the floor, that impact the signal attenuation.
- Plan all APs in sequence.
- Export the floor map as a PDF.

Add a Floor with a Map File

When you create a floor, you can include a floor map at the same time. The following topics help you understand the different floor creation methods depending on the floor map file type that you use. Procedures for each method are also provided.

Floor Map Creation Methods

To view a wireless map, first you need to create or import a floor map:

- **Create a Floor Map:** To create a floor map from scratch, you need to manually create all of the floor elements, such as the walls and shelving, for them to be represented in the wireless map. For details, see [2D Floor Map Devices and Overlay Objects, on page 145](#).
- **Import a CAD file:** When you use a CAD file (DXF or DWG file type) to import the floor map, Cisco DNA Center imports the CAD layers and allows you to specify which layers appear as floor elements in the wireless map.

Because the computation of a 3D heatmap requires significant computing power, we recommend that you include only the CAD layers that contribute significantly to the heatmap computation. You should include enough information to get an accurate heatmap, but not unnecessary information that overloads the computation process and delays the heatmap display.

Cisco DNA Center takes these initial steps to minimize the time it takes to generate a heatmap:

- Restricts the maximum number of walls for 2D and 3D maps. The maximum number of walls for a 3D heatmap is 3000, after optimization. If your CAD file contains more, Cisco DNA Center alerts you and preserves the 3000 most relevant walls (based on the length of the wall multiplied by its attenuation).

The maximum number of walls for a 2D heatmap is 300, after optimization. If your CAD file contains more, Cisco DNA Center alerts you and preserves the 300 most relevant walls (based on the length of the wall multiplied by its attenuation).

- Automatically removes small obstructions (under 0.75 ft) and the second sides of the walls, leaving only one side per wall. (Cisco DNA Center applies an attenuation value for each wall, not for each side of a wall.)

When deciding which layers and elements to import, focus on obstacles that create the most attenuation. In principle, the longer and thicker a wall is, the higher its attenuation. Low walls, like cubicles, and narrow walls, like columns, have low attenuation and have little effect on the heatmap. Even if the material of an obstacle is heavy, the attenuation is not significant, because the signal can radiate around the obstacle. Likewise, if you are not interested in the coverage outside of a building, do not include external walls or windows. Doing so provides better 3D visualization of the inside of the building.

If your CAD file does not have walls in specific layers, but has walls mixed with other elements, do not select them for import. You can add walls manually later. For information, see [Add, Edit, and Remove Walls, on page 160](#).

Block inserts and proxy entities cannot be imported. Please make imported layers contain only native elements like lines, polylines, arcs, and so on.

For the procedure, see [Add a Floor with a CAD Map File, on page 141](#).

- **Import a non-CAD image file:** You can use JPG, GIF, PNG, or PDF files to import the floor plan. Typically, this type of file is used to create 2D floor maps. However, you need to manually create the floor elements, such as the walls and shelving, for them to be represented in the wireless map. For the procedure, see [Add a Floor with a Non-CAD Map File, on page 142](#).
- **Import a Ekahau Pro Project plan:** You can import Ekahau project data, such as the obstacles, APs, and more, to create a wireless map. For the procedure, see [Import an Ekahau Project to Cisco DNA Center, on page 130](#).

Guidelines for Image Files to Use in Maps

Follow these guidelines to use map image files:

- Use a graphical application that can save the map image files to any of these formats—.jpg, .gif, .png, .pdf, .dxf, and .dwg.
- Map image files can be of any size. Cisco DNA Center imports the full definition of the original images to its database, but during display, it automatically resizes them to fit the workspace.
- Obtain the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during map import.
- Avoid using floor map images with rotation metadata, because the images might not render correctly when synced to CMX or Cisco Spaces. Although the floor map images might be in formats that are supported by Cisco DNA Center, the ways in which certain tools add the metadata can be rendered differently. For example, an image file with rotation metadata that is opened in three different applications might render horizontally in two applications and vertically in the other.

Add a Floor with a CAD Map File

To view a wireless map, you must create a floor map. You can use CAD files (DXF or DWG file types) to create a floor map.

For 2D floor maps, you must choose the CAD layers that you want to be displayed in the 2D view. For 3D floor maps, Cisco DNA Center imports CAD layers as walls, shelving, obstacles, and other elements in the map.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, hover your cursor over the ellipsis ... next to the building and choose **Add Floor**.
- Step 3** In the **Floor Name** field, enter a name for the floor.
- Step 4** From the **Type (RF Model)** drop-down list, choose the RF model to apply to the floor. The RF model determines how the RF is calculated based on the characteristics of the floor.
- Step 5** Drag and drop the CAD file (the DXF or DWG file type) to the **Floor Image** area.
- Note** By default, overlays are not displayed after you import a map. So, after you import a floor plan, make sure that you enable the overlay visibility. From the map toolbar, click **View Options**. From the right pane, expand **Overlay Objects** and click the toggle button for each object you want to display.
- Step 6** In the **Floormap** dialog box, choose the CAD layers that you want to be displayed as floor elements in the map:

- a) For the **2D** column, check the check boxes of the CAD layer that you want to be displayed in the 2D view.
- b) For the **3D Wall/Shelving Type** column, use the drop-down list to choose a CAD layer that specifies the type of the wall or shelving.

Note For a layer to appear in the 3D view, a **3D Wall/Shelving Type** value is required. The wall/shelving type affects attenuation and how the heatmap is calculated. For more information, see [Floor Map Creation Methods](#), on page 140.

- c) Click **Use Selected Layers**.

Step 7 Enter the floor map dimensions in the **Width**, **Length**, and **Height** fields.

Step 8 Click **Add**.

By default, the map is displayed with a grid. To turn the grid off or on, use the **Show Grid** toggle button at the bottom-left side of the map.

Note After you import a floor plan, make sure that you enable the overlay visibility. (From the floor, click **View Options** and enable the overlay toggles in **Overlay Objects**). By default, overlays are not displayed after you import a map.

Add a Floor with a Non-CAD Map File

You can use non-CAD files (JPG, GIF, PNG, or PDF file types) to create a floor map. However, when using a non-CAD file, the 3D floor elements, such as walls and shelvings, cannot be imported, and you must add them manually later. For more information, see [2D Floor Map Devices and Overlay Objects](#), on page 145.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, hover your cursor over the ellipsis ... next to the building and choose **Add Floor**.

Step 3 In the **Floor Name** field, enter a name for the floor.

Step 4 From the **Type (RF Model)** drop-down list, choose the RF model to apply to the floor. The RF model determines how the RF is calculated based on the characteristics of the floor.

Step 5 Drag and drop the non-CAD file (JPG, GIF, PNG, or PDF file type) onto the **Floor Image** area.

Note Ensure to provide the precise dimensions of floors that are in PDF format, because the image width and height ratio cannot be extracted from them.

Step 6 Click **Add**.

The floor map is created.

Note After you import a floor plan, make sure that you enable the overlay visibility. (From the floor, click **View Options** and enable the overlay toggles in **Overlay Objects**). By default, overlays are not displayed after you import a map.

Step 7 From the map toolbar, click **Add/Edit**.

Step 8 To add walls as a 3D floor element, do the following:

- a) From the map toolbar, click **Add/Edit > Overlays > Walls**.
- b) From the left pane of the map, click the wall type that you want to add.

If the wall type is not in the list, click **Add Wall Type** to create a new wall type.

- c) Use the drawing tool to create a wall on the map:
 - Click where you want to begin the wall. Then move your cursor to the next point and click again. Continue this process until you have created the wall in the shape you want.
 - To finalize the wall, double click where you want the wall to end. To cancel the drawing, right-click the map.
 - To change the type of an existing wall, right-click the shape and choose **Change Type**.
 - To move an existing wall, drag and drop the shape to the new location.
 - To remove an existing wall, right-click the shape and choose **Delete**.

Figure 4: Adding a Wall with the Drawing Tool

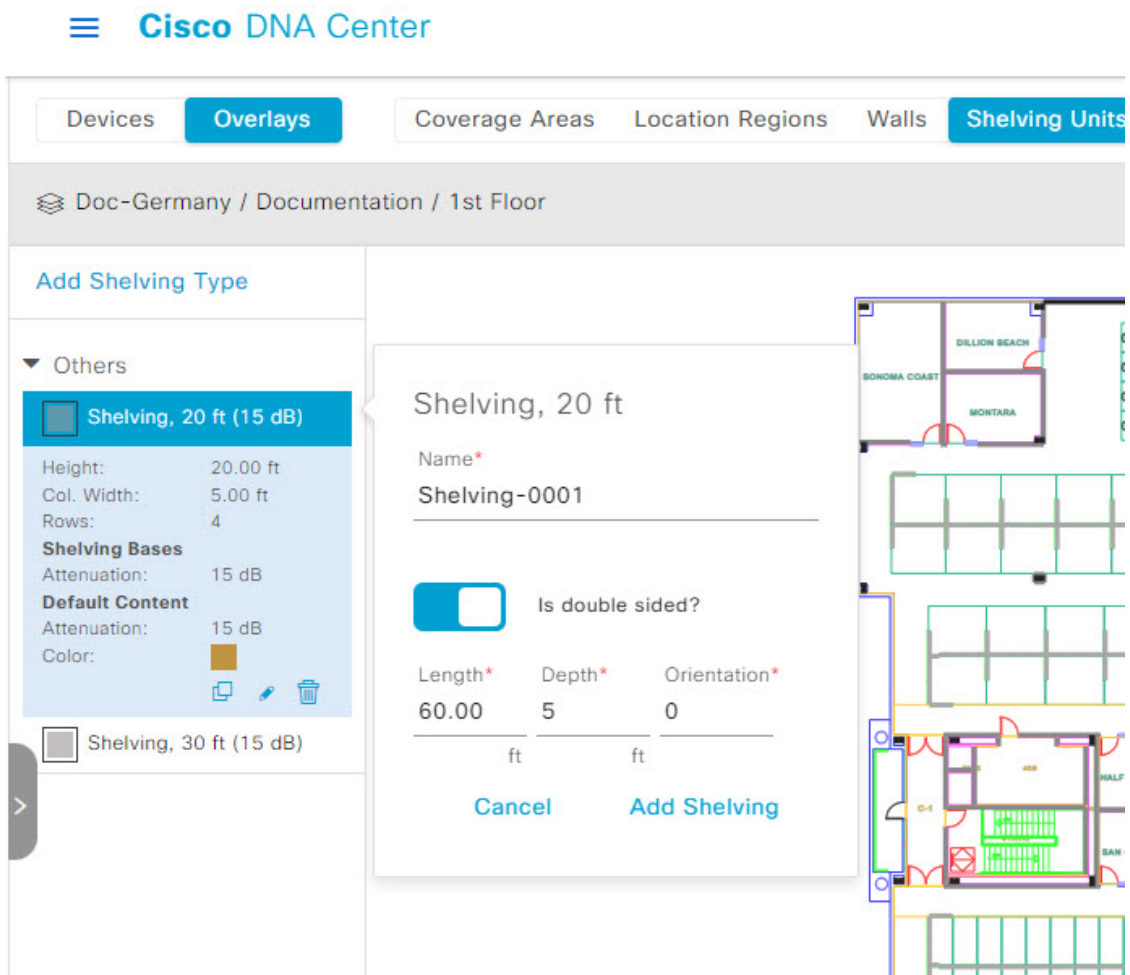


Step 9

To add shelving units as a 3D floor element, do the following:

- a) In the map toolbar, click **Shelving Units**.
- b) In the left pane of the map, click the shelving type that you want to add.
 - In the **Shelving** dialog box, you can edit the name, dimensions, and orientation of the shelving type. Orientation refers to the angle of the shelving, for example, 0 means that the shelving is vertical and parallel to the y axis.
 - If a shelving type is not in the list, click **Add Shelving Type** to create a new shelving type.

Figure 5: Choosing a Shelving Type to Add



- c) In the **Shelving** dialog box, click **Add Shelving** to add the shelving to the floor map.
- d) Drag and drop the shelving to move it to a location on the floor map.
- e) Right-click the shelving and choose one of the following actions:
 - **Edit**: Edit the name, dimensions, and orientation of the shelving.
 - **Clone**: Create a copy of the shelving.
 - **Array**: Create an array of shelving by specifying the number of shelves and the distance between them.
 - **Delete**: Remove the shelving from the floor map.

Step 10 When you're done, click **Save** in the map toolbar.

Work with 2D Maps

2D maps are primarily used to configure elements on a floor map and view heatmaps.

Using 2D maps, you can add floor map elements and overlays. While viewing a 2D map, you can manipulate the display of the various elements and overlays. You can also filter device data and identify wireless interferers.

Cisco DNA Center calculates the strength and quality of wireless signals. These RF predictions are commonly known as heatmaps, because they show the relative intensity of the RF signals on the 2D wireless coverages area map.

2D Floor Map Devices and Overlay Objects

In 2D maps, you can configure devices and overlay objects on your floor maps.

Devices

- **APs:** An access point (AP) serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In 2D maps, an AP represents an actual, installed device. For a list of APs that Cisco DNA Center supports, see the [Cisco DNA Center Compatibility Matrix](#).
- **Planned APs:** Planned APs are representations of APs that have not been installed yet. By placing planned APs on a map, you can envision your wireless network RF coverage and make changes before you actually install the APs.
- **Sensors:** A sensor is a dedicated Cisco Aironet 1800S Active Sensor that gets bootstrapped using Cisco PnP. After it obtains the Assurance server reachability details, it communicates directly with the Assurance server. For more details, including information about sensor tests, see the [Cisco DNA Assurance User Guide](#).

Overlay Objects

- **Coverage Areas:** By default, any area defined as part of a floor map is considered as a wireless coverage area. However, if you have a building that is nonrectangular or you want to mark a nonrectangular or polygon-shaped area on a floor, you can use the **Coverage Areas** drawing tool to create a coverage area.
- **Openings:** An opening, also called an atrium, is an open-air or skylight-covered area within a building. An opening can extend through multiple floors and can affect wireless signal coverage areas.
- **Location Regions:** Location regions define areas that are included in or excluded from the computation of heatmaps. Inclusion areas are included in the calculations, and exclusion areas are not included. For example, you might want to exclude areas such as openings, atriums, or stairwells within a building, but include a work area, such as cubicles, labs, or manufacturing floors.
- **Walls:** Walls are exterior or interior vertical structures in a building and can be made of different materials and thicknesses. As such, they affect how heatmaps are calculated.
- **Shelving Units:** Shelving units are obstacles that affect signal attenuation. A high-ceiling warehouse is an example of a location with shelving units.
- **Markers:** A marker identifies a location on a map. When you create a marker, you can name it and position it to help you identify it later.

- **GPS Markers:** When integrated with Cisco DNA Center, location services, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), use GPS markers to calculate the approximate geographical location of clients.
- **Align Points:** Align points are markers that are used to position multiple floors that have different physical shapes. In 3D maps, floors are aligned at the top-left corner of the map (point 0,0). If you manage each floor independently, the misalignment is not a problem. However, to use some of the features of 3D maps, the floors need to be aligned as they are in reality. To compensate this misalignment, you can insert one or more align points on two or more floors, so that the floors align properly one on top of the other in a 3D map.

Work with APs on a Floor Map

Cisco DNA Center computes heatmaps for the entire map that show the relative intensity of the Radio Frequency (RF) signals in the coverage area. For 2D wireless maps, the heatmap is only an approximation of the actual RF signal intensity because it does not consider the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Follow these guidelines while placing APs on the floor map:

- Place APs along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. APs placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other APs.
- Location accuracy can be improved by increasing overall AP density and moving APs close to the perimeter of the coverage area.
- In long and narrow coverage areas, avoid placing APs in a straight line. Stagger them so that each AP is more likely to provide a unique snapshot of the device location.
- Although the design provides enough AP density for high-bandwidth applications, location suffers because each AP view of a single device is not varied enough. Therefore, location is difficult to determine. Move the APs 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.
- For optimal heatmap visibility on floor maps, configure the AP height to approximately 10 feet (3 meters) or lower.

Export Bulk APs from Cisco Prime Infrastructure and Import into Cisco DNA Center

Cisco DNA Center allows you to import, assign, and position a collection of access points to the floor map. If you have an existing collection of access points on Cisco Prime Infrastructure, you can import it into Cisco DNA Center, saving time and effort spent in importing, assigning, and positioning access points to the floor map.

This procedure describes how to export an existing collection of access points from Cisco Prime Infrastructure, and import into Cisco DNA Center.

Before you begin

- To perform the following task, you must be a **Super Admin** or **Network Admin**.
- Make sure that you have APs in your inventory. If not, discover them using the **Discovery** feature.

- Add and position APs on a floor map.
- The area, building, and floor must be present in the site hierarchy.

-
- Step 1** Export the bulk AP positions from Cisco Prime Infrastructure as a CSV file to your workstation.
- Step 2** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 3** From the left hierarchy tree, hover your cursor over the ellipsis ... next to the site and choose **Import Bulk AP**.
- Step 4** In the **Import Bulk AP** pop-up window, drag and drop the AP file, or click **Choose a file** to select the file from your workstation.
- Note**
- To manually create the **AP Positions** CSV file with Prime Template, export a Prime Template to your workstation by clicking **Download Prime Template**. Prime Template does not support nested files.
 - To manually create the **AP Positions** CSV file with Cisco DNA Template, export a Cisco DNA Template to your workstation by clicking **Download Template**. Cisco DNA Template supports nested files.
- Wait for the CSV file to download. The CSV file contains information about AP positions of various sites in the network.
- Step 5** Click **Import**.
- The **Import Summary** window is displayed.
- The **Information** tab shows the list of successfully imported APs.
 - Click the **Warning** tab to see the list of warnings.
 - Click the **Error** tab to see the list of errors.

Add APs to a Map

This procedure describes how to add APs to a map.

Before you begin

Make sure that you have Cisco APs in your inventory. If not, discover them using the Discovery feature. See [Discovery Overview, on page 37](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** From the map toolbar, click **2D > Add/Edit > APs**.
- Step 4** In the map left pane, click **Add APs**.
- Step 5** In the **Add APs** slide-in pane, do one of the following:
- **To add a single AP:** Click **Add** next to an AP that you want to add.
 - **To add multiple APs:** Check the check boxes next to APs you want to add and click **Add Selected**.

Note You can search for APs using the search option available. Use the **Filter** field to search for APs using the AP name, MAC address, model, or Cisco Wireless Controller. The search is case-insensitive. The search results appear in a table. Click **Add** to add one or more of these APs to the floor area.

In edit mode, newly added APs appear in the **Unpositioned** category in the map left pane. For more information, see [Position an AP on a Map, on page 150](#).

Step 6 After adding the APs to a floor, close the **Add APs** window.

What to do next

When you add an AP to a map, the wireless map automatically stores the following data even after the AP is deleted from the inventory:

- AP name
- AP MAC address
- Current site of the AP
- Current position of the AP on the map



Note If you delete the corresponding site from the network hierarchy, the stored AP data is also removed.

When you delete the wireless controller with all its managed APs from the inventory, Cisco DNA Center displays a planned AP icon for the corresponding APs on the map. For more information, see [AP Icon Legend, on page 170](#).

If the same AP is rediscovered in the inventory later, Cisco DNA Center automatically places it back on the map at the same site and position even if a different wireless controller manages it.

To remove the AP data from the map when the AP is deleted from the inventory, you can do one of the following:

- Before deleting the wireless controller from the inventory, assign the corresponding APs to the **Global** site. For more information, see [Add a Device to a Site, on page 90](#).
- After deleting the wireless controller from the inventory, remove the corresponding planned APs from the map. For more information, see [Remove APs from a Map, on page 155](#).

Add Planned APs to a Map

This procedure shows you how to use the AP Model Catalog feature to add a planned AP to a floor and configure its model, antenna type, azimuth, and elevation orientation. Using the planned AP that you just created and placed, you can add more planned APs with the same properties.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D > Add/Edit > APs**.

Step 4 In the left pane of the map, in the **AP Models** area, click the AP model of the planned AP to add.

Note If the AP model that you want to add is not listed, click **Add Model** to choose the AP model to add to the list.

Step 5 On the floor map, click the location where you want to place the planned AP.

A planned AP of the selected model is added to the floor map and the **Edit Planned AP** slide-in pane is displayed to the right, with an AP name added to it by default.

Step 6 In the **Edit Planned AP** slide-in pane, click the gear icon that is located next to the **AP Name** field.

The **Name pattern** dialog box is displayed.

Step 7 When you add the first AP to the floor, make sure that you enter a valid name pattern, for example, SJC-BLD21-FL2-AP####, and then click **Set name pattern**.

Note The planned APs must be unique within Cisco DNA Center. So, make sure that the name pattern identifies the floor.

The #### in the name pattern is replaced by numbers in the **AP Name**, for example, SJC-BLD21-FL2-AP0001, SJC-BLD21-FL2-AP0002, and so on.

Step 8 From the **Antenna** drop-down list, choose the appropriate antenna type, including dual antennas, for the AP.

Note The antenna image reflects the selected antenna.

Step 9 Depending on the antenna type, enter the **Azimuth** and **Elevation** orientation, in degrees.

Step 10 Perform the following actions, as needed:

- To add another planned AP with the same properties as that of the planned AP that you just added, on the floor map, click a location where you want to position the new AP.
A new AP icon is displayed on the map with all of the properties inherited and the AP name appended, for example, BLD1-AP0002-TX.
- To add more planned APs with the same properties and appended AP name, click the floor map.
- To stop adding planned APs to the floor map, press **Esc** or right-click the floor map.
- To reposition the planned APs, drag and drop them to the appropriate location in the floor map.
- To delete a planned AP, right-click the AP icon and click **Delete**.
- To edit a planned AP, right-click the AP icon and click **Edit**.

Step 11 In the map toolbar, click **Save**.

Assign Actual APs to Planned APs

After you install the actual APs in your wireless network, you can assign them to the planned APs on your map. This procedure describes how to assign planned APs to actual APs.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

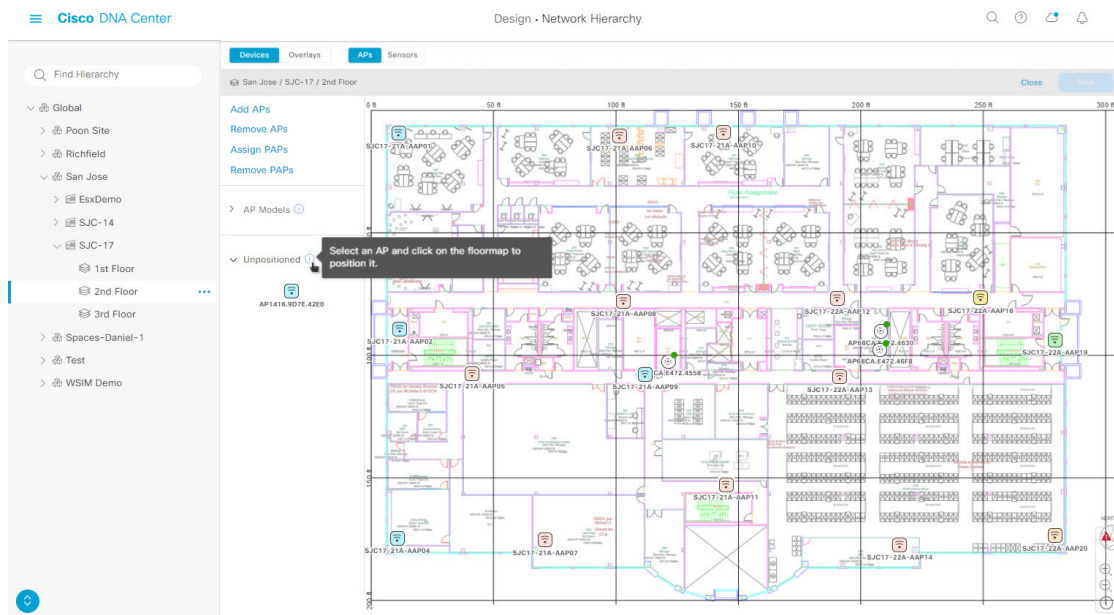
- Step 3** In the map toolbar, click **2D > Add/Edit > APs**.
- Step 4** In the left pane of the map, click **Assign PAPs**.
- Step 5** On the floor map, click a planned AP.
- Step 6** In the **Assign Planned APs** slide-in pane, check the check box next to the AP that you want to assign.
- Step 7** Click **Assign**.
- Step 8** In the map toolbar, click **Save**.

Position an AP on a Map

After adding APs to a floor, you must position them on the map. This procedure shows you how to position APs on a map.

- Step 1** Click the menu icon (**≡**) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > APs**.
- Step 4** From the **Unpositioned** category in the left pane of the map, click an AP.

Figure 6: Unpositioned APs



- Step 5** To position the AP, do one of the following:
- Click the location on the floor map where you want to position the AP.
 - In the **Edit AP** slide-in pane, enter the **x** and **y** coordinates in the corresponding fields.
 - Draw three points on the floor map and position the AP by using the selected points. To draw three points, do the following:
 - a. In the **Edit AP** slide-in pane, click **Position by 3 points**.

- b. To define the points, click anywhere on the floor map to draw the first point. Click again to finish drawing the point.
A dialog box is displayed to set the distance to the first point.
 - c. Enter the distance, in meters, and click **Set Distance**.
 - d. Define the second and third points similarly, and click **Save**.
- Define two walls on the floor map and position the APs between the defined walls. This method helps you to know the position of APs between the two walls.
 - a. In the **Edit AP** slide-in pane, click **Position by 2 walls**.
 - b. To define the first wall, click anywhere on the floor map to start drawing the line. Click again to finish drawing the line.
A dialog box is displayed to set the distance to the first wall.
 - c. Enter the distance in meters and click **Set Distance**.
 - d. Define the second wall similarly and click **Save**.
The AP is placed based on the defined distance between the walls.

Step 6 In the map toolbar, click **Save**.

Note If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, you can view the location of clients on the heatmap. See [Create Cisco CMX Settings, on page 266](#).

Reposition an AP on a Map

After you position APs on a map, you can reposition them. This procedure shows you how to reposition an AP on a map.



Note You can perform this task in a 2D or 3D map.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 For 2D, do the following:

- a) In the map toolbar, click **2D > Add/Edit**.
- b) On the map, drag and drop the AP to the new position.

Step 4 For 3D, do the following:

- a) In the map toolbar, click **3D > Add/Edit**.
- b) On the map, right click the AP and choose **Move**.
- c) On the map, drag and drop the AP to the new position.

Step 5 In the map toolbar, click **Save**.

Edit an AP

This procedure shows you how to change the configuration of a single AP. To change the configuration of multiple APs at the same time, see [Edit Multiple APs, on page 153](#).



Note You can perform this task in a 2D or 3D map.

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 For 2D, do the following:

- a) In the map toolbar, click **2D > Add/Edit**.
- b) On the map, right-click the AP and choose **Edit**.

Step 4 For 3D, do the following:

- a) In the map toolbar, click **3D > Add/Edit**.
- b) On the map, right-click the AP and choose **Details**.

Step 5 In the **Edit AP** slide-in pane, change any of the following AP settings, as needed:

- **AP Name** or **Planned AP Name**: Name of the AP.
- **MAC Address**: MAC address of the selected AP.
- **AP Model**: Model of the selected AP.
- **x**: X-axis coordinate of the AP.
- **y**: Y-axis coordinate of the AP.
- **AP Height**: Height of the AP.
- **Antenna**: Antenna type for this AP.

Note For external APs, you must select an antenna. If you don't select an antenna, the AP will not be present on the map.

- **Azimuth**: Angle of the antenna, measured relative to the x axis, clockwise. The azimuth range is from 0 through 360. In Cisco DNA Center, pointing right is 0 degrees or 360 degrees; pointing down is 90 degrees.

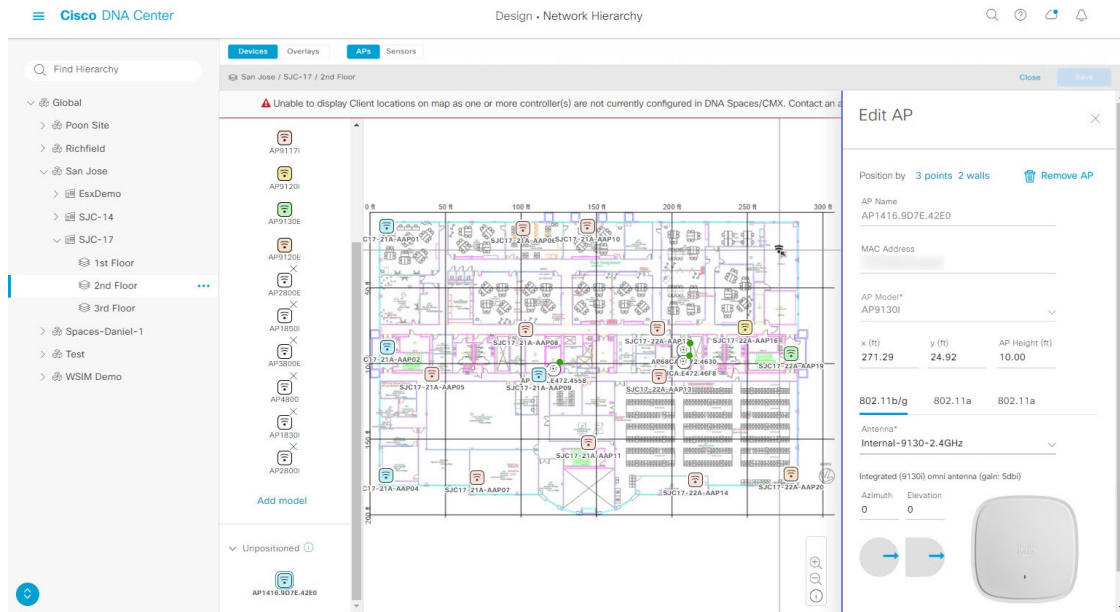
You can manually enter the value or use the blue arrow under the field to change the value.

Note For omnidirectional antennas, the azimuth is not relevant if the elevation is 0.

- **Elevation**: in degrees. You can manually enter the value or use the blue arrow under the field to change the value.

Note For APs and antenna models that are designed to be placed on a ceiling, 0 elevation means pointing down. For APs and antenna models that are designed to be placed on a wall, 0 elevation means pointing horizontally and negative values means pointing down.

Figure 7: Edit AP Slide-In Pane



Step 6 In the map toolbar, click **Save**.

Edit Multiple APs

When you select only one AP, you can change all editable attributes. However, when you select multiple APs, only some attributes are editable, as follows:

- When the selected devices have the same value for an attribute, the value is displayed. Otherwise, the value is blank. In either case, if you change the value, the new value is applied to all the selected devices.
- When the selected APs have the same model number and radios (number of radios and operating band), the antennas are editable. Otherwise, they are not editable.
- You can change the model numbers of planned APs, but not added APs. So, if you select an AP, the model number is not editable.
- Because bulk changes affect more devices, they do not take effect immediately. You must click **Apply** to apply your changes.

This procedure shows you how to update the editable attributes for multiple APs at the same time.



Note You can perform this task in a 2D or 3D map.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 Do one of the following:

- For 2D, in the map toolbar, click **2D > Add/Edit**.
- For 3D, in the map toolbar, click **3D > Add/Edit**.

Step 4 Select the APs, using one of the following methods:

- Click the first device, then press and hold the **Shift** key while you click the rest of the devices.
- In the map navigation toolbar, click **Select by rectangle**. Then click an area of the map and drag the highlighted rectangle to select APs in a contiguous area. All the highlighted APs within the rectangle are selected.

To deselect APs, use one of the following methods:

- To deselect a single AP, press and hold the **Shift** key while you click the AP.
- To deselect all APs except one, click the AP you want to remain selected. All others are deselected.
- To deselect all APs, press the **ESC** key or close the **Edit** pane.

Step 5 In the **Edit AP** slide-in pane, configure the settings, as available:

- **AP Name** or **Planned AP Name**: Name of the AP.
- **MAC Address**: MAC address of the selected AP.
- **AP Model**: Model of the selected AP.
- **x**: X-axis coordinate of the AP. You can manually enter the value.
- **y**: Y-axis coordinate of the AP. You can manually enter the value.
- **AP Height**: Height of the AP. You can manually enter the value.
- **Antenna**: Antenna type for this AP.

Note For external APs, you must select an antenna, or the AP will not be present in the map.

- **Azimuth**: Angle of the antenna, measured relative to the x axis, clockwise. The azimuth range is from 0 through 360. In Cisco DNA Center, pointing right is 0 degrees or 360 degrees; pointing down is 90 degrees.

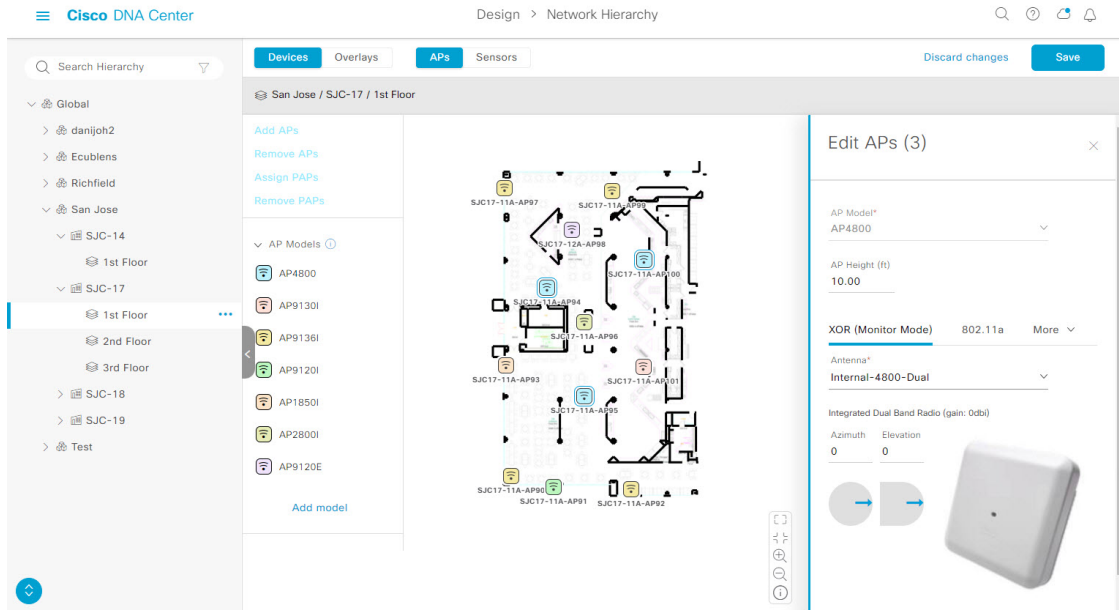
You can manually enter the value or use the blue arrow under the field to change the value.

Note For omnidirectional antennas, the azimuth is not relevant if the elevation is 0.

- **Elevation**: in degrees. You can manually enter the value or use the blue arrow under the field to change the value.

Note For APs and antenna models that are designed to be placed on a ceiling, 0 elevation means pointing down. For APs and antenna models that are designed to be placed on a wall, 0 elevation means pointing horizontally and negative values means pointing down.

Figure 8: Edit Multiple APs Slide-In Pane



Step 6 In the map toolbar, click **Save**.

Remove APs from a Map

This procedure shows you how to remove APs and planned APs (PAPs) from a map.

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit**.
- Step 4** To remove APs (including planned APs), do the following:
- Click the AP, or to select multiple APs, click the first AP and while pressing the **Shift** key, click the rest of the APs.
 - In the **Edit** pane, click **Remove Selected**.
- Step 5** In the map toolbar, click **Save**.

Work with Sensors on a Floor Map

The following topics show you how to add sensors to floor maps and position, reposition, and delete them, if needed.

For more information about sensors, see [2D Floor Map Devices and Overlay Objects](#), on page 145.

Add Sensors to a Map

This procedure shows you how to add sensors to a map.

Before you begin

Make sure you have the Cisco AP 1800S sensor in your inventory. The Cisco Aironet 1800s Active Sensor must be provisioned using Plug and Play for it to show up in the Inventory. See the "Provision the Wireless Cisco Aironet 1800s Active Sensor" topic in the [Cisco DNA Assurance User Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Sensors**.
- Step 4** In the **Add Sensors** slide-in pane, check the check boxes of the sensors that you want to add. Alternatively, click **Add** next to the sensor row.
- Note** You can search for specific sensors using the **Filter** field. Search using the name, MAC address, or model of a sensor. The search is not case-sensitive. The results are displayed in the table. Click **Add** to add one or more of these sensors to the floor area.
- Newly added sensors are displayed in the **Unpositioned** category in the left pane of the map in edit mode.
- Step 5** In the map toolbar, click **Save**.
-

Position Sensors on a Map

Newly added sensors are displayed in the **Unpositioned** category in the left pane of the map in edit mode. This procedure shows you how to position a sensor after initially adding it.

Before you begin

Sensors must be added to the map before they can be positioned. For information, see [Add Sensors to a Map, on page 155](#)


-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Sensors**.
- Step 4** In the left pane of the map, click a sensor in the **Unpositioned** category to position the sensor.
- Step 5** On the floor map, click the location where you want to position the sensor.
- You can use the **x**, **y**, and **sensorHeight** fields in the **Sensor Details** slide-in pane to enter the exact x, y, and z coordinates for the sensor.
- Step 6** In the map toolbar, click **Save**.
-

Reposition a Sensor on a Map

After you position sensors on a map, you can reposition them. This procedure shows you how to reposition a sensor on a map.




Note You can perform this task in a 2D or 3D map.

-
- Step 1** Click the menu icon () and choose **Design > Network Hierarchy**.
 - Step 2** From the left hierarchy tree, choose a floor.
 - Step 3** In the map toolbar, click **2D** or **3D**.
 - Step 4** In the map toolbar, click **Add/Edit**.
 - Step 5** On the map, drag and drop the sensor to the new position.
 - Step 6** In the map toolbar, click **Save**.
-

Remove Sensors from a Map


This procedure shows you how to remove sensors from a floor map.

-
- Step 1** Click the menu icon () and choose **Design > Network Hierarchy**.
 - Step 2** From the left hierarchy tree, choose a floor.
 - Step 3** In the map toolbar, click **2D > Add/Edit**.
 - Step 4** To remove sensors, do the following:
 - a) Click the sensor, or to select multiple sensors, click the first sensor and while pressing the **Shift** key, click the rest of the sensors.
 - b) In the **Edit** pane, click **Remove**.
 - Step 5** In the map toolbar, click **Save**.
-

Add, Edit, and Remove Coverage Areas

This procedure shows you how to mark a nonrectangular or polygon-shaped area as a coverage area on a floor map.

For more information about coverage areas, see [2D Floor Map Devices and Overlay Objects, on page 145](#).

-
- Step 1** Click the menu icon () and choose **Design > Network Hierarchy**.
 - Step 2** From the left hierarchy tree, choose a floor.
 - Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Coverage Areas**.
 - Step 4** To add a coverage area, do the following:
 - a) In the **Coverage Area** dialog box, enter a name for the coverage area in the field.
 - b) Click **Add Coverage**.
 - c) Click on the map to create a point and initiate the drawing tool.
 - d) Continue creating points to define the coverage area shape.

Note The coverage area shape must have at least three points. Click and drag a point to redefine the coverage area shape.

e) Double-click to exit the drawing tool and finalize the coverage area shape.

Step 5 To edit a coverage area, do the following:

- a) In the map toolbar, click **Add/Edit > Coverage Areas**.
- b) To redefine the shape of a coverage area, click and drag a point.
- c) To edit a coverage area name, right-click the coverage area and choose **Edit**.

Step 6 To delete a coverage area, do the following:

- a) In the map toolbar, click **Add/Edit > Coverage Areas**.
- b) Right-click the coverage area and choose **Remove**.

Step 7 In the map toolbar, click **Save**.

Add, Edit, Copy, and Remove Openings

Creating an opening is similar to creating an open space or atrium on a floor. On multifloor buildings, typically the opening extends vertically through multiple floors. This procedure shows you how to add, edit, and remove openings on a floor map. It also shows you how to copy openings to other floors.

For more information about openings, see [2D Floor Map Devices and Overlay Objects, on page 145](#).

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D > Add/Edit > Overlays > Openings**.

Step 4 To add an opening, do the following:

- a) From the left pane of the map, click **Opening**.
- b) Click on the map to create a point and initiate the drawing tool.
- c) Continue creating points to define the opening shape.

Note The opening shape must have at least three points. Click and drag a point to redefine the opening shape.

d) Double-click to exit the drawing tool and finalize the shape.

Step 5 To edit an opening, do the following:

- a) In the map toolbar, click **Add/Edit > Openings**.
- b) To redefine the shape of an opening, click and drag a point.
- c) To move an opening, click inside the shaded area. Then, drag and drop the opening where you want to place it.

Step 6 To copy an opening from one floor to another, do the following:

- a) In the map toolbar, click **Add/Edit > Openings**.
- b) Right-click the opening and choose **Copy to other floors**.
- c) In the dialog box, check the check boxes next to the relevant floors.
- d) Click **Copy**.
- e) Click **Close**.

- Step 7** To remove an opening, do the following:
- In the map toolbar, click **Add/Edit > Openings**.
 - Right-click the opening and choose **Remove**.
- Step 8** In the map toolbar, click **Save**.
-

Add, Edit, and Remove Location Regions

Location regions are areas on the map that are either included in or excluded from the heatmap calculation. The following topics show you how to add, edit, and remove location regions.

Add, Edit, and Remove an Inclusion Region

This procedure shows you how to add, edit, and remove an inclusion region. Use the following guidelines to define an inclusion region on a floor map:

- Inclusion regions can be any polygon-shaped area 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 area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.

For more information about inclusion regions, see [2D Floor Map Devices and Overlay Objects, on page 145](#).

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Location Regions**.
- Step 4** In the left pane of the map, click the **Inclusion** icon.
- Step 5** To create an inclusion region, use the drawing tool:
- Click the map to create a point where you want the inclusion region to begin.
 - Move the cursor to the next point and click again.
 - Continue creating points to define the inclusion region shape.
 - To finalize the shape, double-click the map.
- Alternatively, from the left pane of the map, click the **Inclusion** icon.
- To exit the drawing tool, double-click the map again.
- Step 6** To edit the location of an inclusion region, drag and drop the shape to the new location.
- Step 7** To remove an inclusion region, right-click the shape and choose **Remove**.
- Step 8** In the map toolbar, click **Save**.
-

Add, Edit, and Remove an Exclusion Region

This procedure shows you how to add, edit, and remove an exclusion region. Use the following guidelines to define exclusion regions on a floor map:

- Exclusion regions can be any polygon-shaped area and must have at least three points.
- Exclusion regions are defined within the borders of an inclusion region.
- You can define multiple exclusion regions on a floor map.

For more information about exclusion regions, see [2D Floor Map Devices and Overlay Objects, on page 145](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Location Regions**.
- Step 4** From the left pane of the map, click the **Exclusion** icon.
- Step 5** To create an exclusion region, use the drawing tool:
- Click the map to create a point where you want the exclusion region to begin.
 - Move the cursor to the next point and click again.
 - Continue creating points to define the exclusion region shape.
 - To finalize the shape, double-click the map.
- Alternatively, from the map left pane, click the **Exclusion** icon.
- To exit the drawing tool, double-click the map again.
- Step 6** To edit the location of an exclusion region, drag and drop the shape to the new location.
- Step 7** To remove an exclusion region, right-click the shape and choose **Remove**.
- Step 8** In the map toolbar, click **Save**.
-

Add, Edit, and Remove Walls

This procedure shows you how to add, edit, move, and remove walls on a floor map.

For more information about walls, see [2D Floor Map Devices and Overlay Objects, on page 145](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D > Add/Edit > Overlays > Walls**.
- Step 4** To add walls, do the following:
- In the left pane of the map, click a wall type from the **Others** or **On this floor** category.
- Note** If a wall type isn't listed, click **Add Wall Type** to create a custom wall type.
- Click the map to create a point where you want the wall to begin.
 - Move the cursor to the next point, where you want to end the wall or where you want to create a corner and click again.
 - Continue creating points to define the wall shape.
 - To end a wall, double-click the map.
- Alternatively, from the left pane, click the wall type.

f) To exit the drawing tool, double-click the map again.

Step 5 To change a wall type, and depending on the wall type also configure its parameters, do the following:

a) Click the wall that you want to change.

The **Wall Type** dialog box opens.

b) From the **Wall Type** drop-down list, choose the type of wall.

c) Configure any other parameters that are appropriate for the new wall type.

d) Click **Update**.

Step 6 To move a wall, do the following:

a) Hover your cursor over the wall that you want to move.

The wall turns black, which means it's selected.

b) Click the wall and drag and drop it to the new location.

Step 7 To remove a wall, right-click the wall and choose **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, Copy, Edit, and Remove Shelving Units

This procedure shows you how to add, copy, edit, and remove shelving units on a floor map.

For information about shelving units, see [2D Floor Map Devices and Overlay Objects, on page 145](#).

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D > Add/Edit > Overlays > Shelving Units**.

Step 4 To add shelving units, do the following:

a) In the left pane of the map, click the shelving type you want to add.

b) In the shelving dialog box, configure the name, dimensions, orientation, and whether the unit is double-sided, or leave the default values. Orientation means the angle of the shelving unit. A shelving unit with an orientation of 0 means that the shelving unit is vertical and parallel to the y-axis.

If a shelving type is not in the list, click **Add Shelving Type** to create a shelving type.

c) Click **Add Shelving**.

The shelving unit is displayed on the map.

d) Drag and drop the shelving unit to its location on the map.

Step 5 To create a copy or an array of a shelving unit, do one of the following:

- To create a copy, right-click the shelving unit and choose **Clone**.

- To create an array, right-click the shelving unit and choose **Array**. Then specify the number of units and the distance between them.


Step 6 To edit the name, dimensions, orientation, and whether it is two-sided, right-click the shelving unit and choose **Edit**.

Step 7 To remove a shelving unit, right-click the shelving unit and choose **Remove**.

Step 8 In the map toolbar, click **Save**.

Add, Edit, and Remove Markers

The following procedure shows you how to add, edit, and remove markers.

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D > Add/Edit > Overlays > Markers**.

Step 4 In the left pane of the map, click the **Markers** icon.

Step 5 In the **Place Markers** dialog box, enter the name for the marker, and click **Add Marker**.

Step 6 To place the marker, click the map where you want to place the marker.

Step 7 To move a marker, hover your cursor over the marker until it turns blue. Then drag and drop it in the new location.

Step 8 To edit a marker, right-click the marker and choose **Edit**.

Step 9 To remove a marker, right-click the marker and choose **Remove**.

Step 10 In the map toolbar, click **Save**.

Add, Edit, and Remove GPS Markers

This procedure shows you how to add, edit, and remove GPS markers. For more information about GPS markers, see [2D Floor Map Devices and Overlay Objects, on page 145](#).



Note The GPS marker is an attribute of the building. You can apply it to all the floors of the building.

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D > Add/Edit > Overlays > GPS Markers**.

Step 4 To add a GPS marker, do the following:

- a) In the left pane of the map, click the **GPS Markers** icon.
- b) On the map, click the location where you want to place the GPS marker.
GPS markers must be positioned inside the outer-perimeter walls, typically at the building corners.
- c) In the **Place Markers** dialog box, enter the name, latitude, longitude, and the x and y coordinates in the appropriate fields.

The latitude and longitude coordinates of the GPS marker located in the northwest corner of a floor must match the building coordinates.

d) Click **Add GPS Marker**.

Step 5 To edit a GPS marker, right-click the GPS marker and choose **Edit**.

Step 6 To remove a GPS marker, right-click the GPS marker and choose **Remove**.

Step 7 In the map toolbar, click **Save**.

Add, Edit, and Remove Align Points

This procedure shows you how to add, edit, and remove align points. For more information about align points, see [2D Floor Map Devices and Overlay Objects](#), on page 145.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D > Add/Edit > Overlays > Align Points**.

Step 4 To add an alignment point, do the following:

- a) In the left pane of the map, click the **Align Points** icon.
- b) On the map, click the location where you want to place the alignment point.

Step 5 To edit the name of an alignment point, do the following:

- a) Right-click the alignment point and choose **Edit**.
- b) Change the name and click **Edit Marker**.

Step 6 To change the location of an alignment point, do the following:

- a) Right-click the alignment point and choose **Edit**.
- b) Click **Edit Marker**.
- c) Drag and drop the alignment point to the new location.

Step 7 To remove an alignment point, right-click the alignment point and choose **Remove**.

Step 8 In the map toolbar, click **Save**.

View a 2D Wireless Floor Map

Use the 2D heatmap to view information about your wireless network.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **2D**.

The wireless 2D map opens.

Step 4 To display specific details about devices, do the following, based on the device type:

- **APs:** The AP icon indicates the number of radios, their frequency and health, overall health score of the device, and the AP name and mode. For more information about interpreting the AP icon, see [AP Icon Legend](#), on page 170.

To display device details, hover your cursor over an AP icon. Information, such as the AP's Rx neighbors, clients, interferers, and health score, is displayed.

For more details about an AP, in the dialog box, click the **Device 360** link.

Note For **Device 360**, the *Assurance - Base* package is required.

- **Mesh APs:** To display device details, hover your cursor over a mesh AP icon. Information, such as mesh, backhaul, and access data, is displayed.
- **Clients:** To display client information, including a link to its associated AP, hover your cursor over or click a client. For more details about a client, in the dialog box, click the **Client 360** link.
- **Sensors:** To view the status and test results of a sensor, click a sensor icon.
- **Switches and Switch Stacks:** To display the member switches of a switch stack, click the arrow next to the switch stack icon. To display the connections between a switch and its associated APs, hover your cursor over the switch or switch stack icon. The map displays a line showing the connections from the switch and its associated APs. You can also identify switch and AP associations by color. APs connected to one specific switch have labels that match the color code on the switch icon.

To display device details, click a switch or switch stack icon. A slide-in pane opens and displays the device details and options for the heatmap display. Under **Select Heatmap**, you can click any of the following radio buttons:

- **All visible switches:** Computes and displays the heatmap for all the switches in the visible map area.
- **This switch:** Computes and displays the heatmap for the selected switch only.
- **Rest of visible switches:** Computes and displays the heatmap for all of the visible switches, except for the selected switch.
- **None:** Does not include any switch in the heatmap computation and heatmap display.

Step 5 To display information about a link, click the link. Depending on the type of link, information such as link health and other statistics are displayed.

For a mesh link, you can perform a link test between two mesh APs.

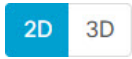

Step 6 Use the tools and options shown in the following figure to gain insights about your wireless network.


Figure 9: 2D Wireless Map Showing Tools and Options


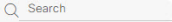


- **Map Toolbar:** In above the map, use the toolbar options to control what's displayed on the heatmap. For details, see [2D Map Toolbar, on page 165](#).
- **View Options Slide-in Pane:** In the slide-in pane, use the view options to customize the heatmap display. For details, see [2D Map View Options, on page 167](#).
- **Navigation Controls:** From the bottom-right corner of the map, use the map navigation controls to manage the heatmap display. For details, see [2D Map Navigation Controls, on page 169](#).

2D Map Toolbar

Item	Description
	Click 2D to view the wireless map in 2D or 3D to view it in 3D.
	Wi-Fi Band Filter: Use this filter to view the heatmap for the 2.4 GHz and 5 GHz Wi-Fi bands.

Item	Description
Add/Edit	<p>Click to enter add and edit mode which allows to do the following:</p> <ul style="list-style-type: none"> • Add, position, and delete floor elements such as: <ul style="list-style-type: none"> • Access points. For details, see Work with APs on a Floor Map, on page 146. • Sensors. For details, see Add Sensors to a Map, on page 155. • Add, edit, and delete overlay objects such as: <ul style="list-style-type: none"> • Coverage areas. For details, see Add, Edit, and Remove Coverage Areas, on page 157. • Location regions. For details, see Add, Edit, and Remove Location Regions, on page 159. • Walls. For details, see Add, Edit, and Remove Walls, on page 160. • Shelving Units. For details, see Add, Copy, Edit, and Remove Shelving Units, on page 161. • Markers. For details, see Add, Edit, and Remove Markers, on page 162. • GPS markers. For details, see Add, Edit, and Remove GPS Markers, on page 162.
Data	<p>Apply filters to the access point, sensor, and client data that appears in the wireless map. For details, see Filter Device Data on a Floor, on page 171.</p>
View Options	<p>Click to open the View Options slide-in pane which contains the view options for the map, devices, and floor map elements.</p>
	<p>Gear Icon: Hover your cursor over the icon for the following options:</p> <ul style="list-style-type: none"> • Recompute: Recomputes the heatmap. • Export: Export the floor map to a PDF or CSV file format. • Edit Floor: Edit the floor details such as its name • Set Scale: Change the scale by doing the following: <ol style="list-style-type: none"> 1. Click on a point and then on another point to specify a known measurement on the map. 2. In the New line length (ft) field, enter the length of the measurement. 3. Click OK. <p>The floor map dimensions are recalculated based on the length of the measurement.</p> • Measure Distance: Measure a distance on the floor map. Click on a point and then another point to specify the distance.

Item	Description
TBD	Full Hierarchy Path: Displays the full navigational path of the floor, including its associated building and site. Click the down arrow to navigate to a different floor.
	Refresh Icon: Click to refresh the device and map data. To the left of the icon is the timestamp for the last refresh
	Search: Use this search field to perform a search for specific floor map elements such as APs, sensors, clients, and so on.

2D Map View Options

To access the 2D map, click the menu icon (☰) and choose **Design > Network Hierarchy**. From the left hierarchy tree, choose a floor, and in the map toolbar, click **2D > View Options**.

The **View Options** slide-in pane opens. Expand the categories to view the settings:

- **Map:** Contains various floor map and heatmap settings:

Item	Description
Show Grid	Click this toggle button to enable or disable a grid on the floor map. The grid provides the dimensions of the floor map.
Map Opacity %	Use this slider to customize the opacity or transparency of the floor map.
Heatmap Type	<p>The heatmap provides a graphical representation of Radio Frequency (RF) wireless data where the values taken by a variable are represented in maps as colors. RSSI heatmaps are computed based on a floor's RSSI prediction model, antenna type, and its orientation.</p> <p>2D heatmaps use fixed transmit powers: 18 dB for 2.4-GHz; 15 dB for 5-GHz; and 5 dB for 6-GHz.</p> <p>3D heatmaps use real-time transmit power of operational APs and 11 dB for planned APs.</p> <p>Use the drop-down list to choose the heatmap type:</p> <ul style="list-style-type: none"> • Operational RSSI: Coverage heatmap, which identifies the wireless signal strength of operational APs. • Planned Heatmap: Hypothetical heatmap that shows the coverage that planned access points would have on a floor. • Operational + Planned RSSI: (3D-only) Coverage heatmap created using both operational and planned APs. 2D maps only show operational AP coverage, so you need to switch to 3D maps to view this combined coverage heatmap. • Client Density: Density of associated clients. • IDS: Heatmap that shows the monitor mode access point coverage provided to the wireless clients on a floor map.
RSSI Cut off (dBm)	Use this slider to set the threshold for the RSSI value to appear on the heatmap. RSSI values that do not meet the threshold are faded.
Heatmap Opacity %	Use this slider to customize the opacity or transparency of the heatmap.

Item	Description
Heatmap Color Scheme	Customize the color scheme for the heatmap. Options are Legacy and Natural .

- **Access Points:** Click this toggle button to enable or disable the AP icons on the floor map.

Expand this category to configure the type of label to display with each AP. Valid label types are **Name**, **AP MAC address**, **IP address**, **Bridge Group Names**, and so on. From the **Display Label** drop-down list, choose a label type.

To display other details about APs, see [View a 2D Wireless Floor Map, on page 163](#).

- **Planned Access Points:** Click this toggle button to enable or disable the appearance of planned AP icons on the floor map.

Expand this category to display labels with the planned AP name. From the **Display Label** drop-down list, choose a label type.

- **Switches and Switch Stacks:** Click this toggle button to enable or disable the appearance of switch or switch stack icons on the floor map.

Expand this category to display labels with the switch name, MAC address, or AP count. From the **Display Label** drop-down list, choose a label type.

To display other details about switches, see [View a 2D Wireless Floor Map, on page 163](#).

- **Sensors:** Click this toggle button to enable or disable the appearance of sensor icons on the floor map.

Expand this category to display labels with the sensor name, MAC address, or AP count. From the **Display Label** drop-down list, choose a label type.




To display other details about sensors, see [View a 2D Wireless Floor Map, on page 163](#).

- **Mesh:** Click this toggle button to enable or disable the appearance of mesh APs on the floor map.

Expand this category to configure options that control how the mesh AP-to-root AP link relationships are displayed:


- **Link Label:** To disable link labels, click the **None** radio button. To display labels for link signal-to-noise ratios, click the **Link SNR** radio button. To display labels for packet error rates, click the **Packet Error Rate** radio button. The link label setting is reflected on the map immediately.
- **Link Color:** To disable link color, click the **None** radio button. To display link signal-to-noise ratios in color, click the **Link SNR** radio button. To display packet error rates in color, click the **Packet Error Rate** radio button.

The link color settings are reflected on the map immediately. See the following table for color definitions.

Link Color	Link Signal Noise Ratio (SNR)	Packet Error Rate (PER)
	Represents an SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
	Represents an SNR between 20 dB and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
	Represents an SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)



- **Mesh Parent-Child Hierarchical View:** Choose which mesh APs to display. From this drop-down list, choose **Select Only Root APs**, **Select up to 1st hops**, **Select up to 2nd hops**, **Select up to 3rd hops**, or **Select All**.
- **Overlay Objects:** Expand this category and click any of the overlay objects to enable or disable the overlay objects on the floor map.
- **Clients:** Click this toggle button to enable or disable the appearance of client icons on the floor map.
Expand this category to display labels with the client name, MAC address, or AP count. From the **Display Label** drop-down list, choose a label type.
To enable or disable clients in close proximity to be grouped together, click the **Show Client Clusters** toggle button.
- **Interferers:** Click this toggle button to enable or disable the appearance of client icons on the floor map.
Expand this category to enable or disable the appearance of a zone of impact from interferers. Click the **Show Zone of Impact** toggle button.
- **Map Properties:** Expand this category to specify the time interval between each auto refresh of map data. From the **Auto Refresh** drop-down lists, choose a time interval.
Additional information is provided depending on the types of devices displayed on the map. For example, when mesh APs are selected to be displayed, the **Map Properties** category shows mesh SNR and PER color charts. You can configure the mesh SNR and PER value ranges and their corresponding colors.
- **Global Map Properties:** Expand this category to change the preferred measurement system. From the **Units of Measure** drop-down list, choose either **Feet** (imperial system) or **Meters** (metric system).
This setting applies to all wireless maps.

2D Map Navigation Controls

To access the 2D map, click the menu icon () and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, choose a floor, and in the map toolbar, click **2D**.

The 2D map navigation controls are located at the bottom-right of the map. For details about the map, see [View a 2D Wireless Floor Map, on page 163](#).

Use the map navigation controls for the following functions:

Map Navigation Controls	Description
	Default Map View: Click to reset the map view to the default.
	Zoom In / Zoom Out: Click the zoom in and out icons to enlarge and reduce the size of the map. Alternatively, you can use your mouse wheel to zoom in and out.

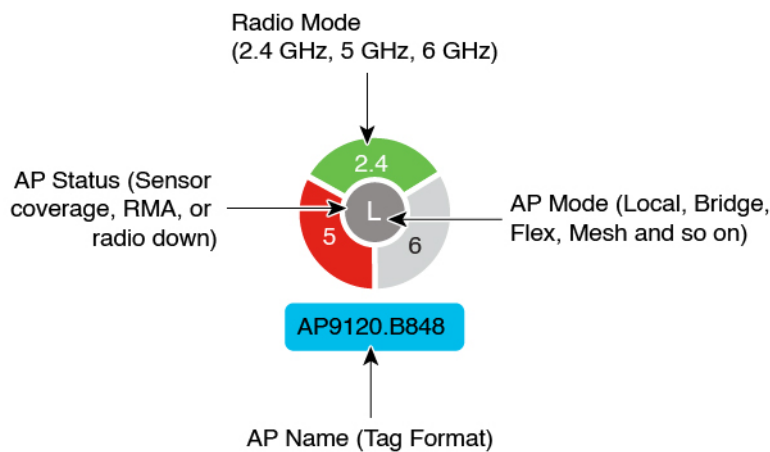
Map Navigation Controls	Description
	Map Legend: Click this icon to view the map legend which describes the map icons such as the device type, average health score, and AP status.
Devices	Access Point Planned AP Sensor Switch Interferer Client Marker
Average Health Score	1-3 4-7 8-10 Unknown Down
AP Status	Covered by sensor Not covered by sensor Covered by RMA or refreshing Radio Down
AP Mode	L: Local M: Monitor F: FlexConnect R: Rogue Detector S: Sniffer B: Bridge C: SE-Connect FB: Flex+Bridge RH: Remote Hybrid Se: Sensor
Radio Status	Not Associated Unreachable Admin Disabled Down Ok Unknown
Radio Mode	2.4, 5 or 6: Servicing clients in that band M: Monitor X: XOR ?: Other

AP Icon Legend

AP icons provide information about the configuration and health of the APs in your network. The circular AP icon is divided into radio bands that are color coded to show the radio status:

- Not Associated
- Unreachable
- Admin Disabled
- Down
- Ok
- Unknown

The following diagram shows all the elements of an AP icon:



465592

Filter Device Data on a Floor

For 2D wireless maps, you can apply various filters to network devices such as access points, sensors, and so on. Based on the filter criteria, the search results appear in a table. Filtering device data is helpful in locating specific devices for floors with many devices.

- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D**.
- Step 4** In the map toolbar, click **Data/Filters**.
- Step 5** In the **Data/Filters** slide-in pane, click the device type that you want to apply a filter to.
- Step 6** Define the filter rules by using the drop-down lists to choose the parameters.
- Step 7** To add more filter rules, click the + icon near the top of the slide-in pane.
- Step 8** When you're done, you can do any of the following:
- To display the results of your filter in the table in the **Data/Filters** slide-in pane, click **Apply Filters to List**.
 - To display the results of your filter in the map, click **Show Selected on Map**.
 - To locate the position of a device on the map, hover your cursor over the device in the table. A line is displayed from the device to its position on the map.

Figure 10: Locating a Device from the Filter Results

The screenshot shows the Cisco DNA Center interface with the 'Planned Access Points' slide-in pane open. The pane displays a table of filtered devices. The table has columns for Name, Radio, and Slot. The filter criteria are: Name contains 4. The table lists 10 devices, all of which are checked. A line connects the selected device 'B1-F1-0004' in the table to its location on the 2D map.

Name	Radio	Slot
B1-F1-0004	802.11a	0
B1-F1-0014	802.11a	1
B1-F1-0024	802.11a	1
B1-F1-0004	802.11a/b/g/n	2
B1-F1-0014	802.11a/b/g/n	0
B1-F1-0024	802.11a/b/g/n	0
B1-F1-0004	802.11b/g	1
B1-F1-0014	802.11b/g	2
B1-F1-0024	802.11b/g	2
B1-F1-0004	802.11b/g	2

- Step 9** To close the slide-in pane and save the filter, click **x**.
- Step 10** To remove applied filters, hover your cursor over the notifications icon and click **Click to clear**.

Identify Wireless Interferers on the Floor Map

This feature is a 2D map feature.

Cisco DNA Center can detect interference and disable the interference source for a specific band on a floor map. Any interference in the 2.4-GHz band disrupts the network traffic of the 802.11 wireless network.

Cisco DNA Center can identify the position, area of impact, and intensity of the interferer.

This procedure shows how to identify network interferers on a floor map.

Before you begin

Ensure that either Cisco Connected Mobile Experiences (CMX) or Cisco Spaces is integrated with Cisco DNA Center. For information, see [About Cisco Spaces Integration, on page 268](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **2D**.
- Step 4** In the **Network Hierarchy** window, click **View Options**.
- Step 5** In the **View Options** window, scroll down and click the **Interferers** toggle button to enable interferers to be displayed on the floor map.
- Step 6** Expand the **Interferers** category and click the **Show Zone of Impact** toggle button to enable the zone of impact of interferers to appear on the floor map.
- Note** By default, **Zone of Impact** is disabled.
- Step 7** On the floor map, hover your cursor over the interferer icon and click the impacted channel to view the interferer device details.
-

Work with 3D Maps

3D maps are primarily used to plan and analyze a wireless network on a floor. As such, there are minimal configuration and edit functions that you can perform in 3D maps.

With 3D wireless maps, you can view a 3D representation of your wireless network. A near real-time predictive model dynamically updates the 3D map to show changes in RF coverage.

Prerequisite

The system you use to compute and display 3D wireless heatmaps must have a Graphical Processing Unit (GPU) installed and enabled on it. For example, if you're using a Windows virtual machine (VM), you need to make sure that it has a GPU.

3D Maps Features and Functionality

Here are some of the unique features and functionality that 3D wireless maps offers:

- Navigate through your wireless network in a 3D environment with a first person view or third person view.
- Gain insights into the areas in your wireless network where service-level agreements (SLAs) are not being met.
- Run an optimizer tool to compute the best AP layout to meet your SLAs.
- View the RF coverage for different elevations and use the **Scanner** tool to view the RF coverage for specific elevations.
- Crop the Key Performance Indicator (KPI) heatmap with the clipping tools.
- Predict the x, y, z coordinates of a specific point on the floor plan with the pin tool to better plan for placement of APs or sensors.
- Visualize floor plan elements, such as walls, in 3D to see how they affect RF coverage and attenuation.
- Simulate your wireless network in various configurations to see how the wireless coverage on a floor is affected. You can save these simulations and open them later to make more changes.
- Modify KPIs, telemetry, and 3D map element settings to customize your map display.

Configure Floor Map Elements and Overlays in 3D Maps

In 3D maps, you are limited to the following configuration and edit functions:

- [Clone an AP, on page 173](#)
- [Edit an AP, on page 152](#)
- [Edit Multiple APs, on page 153](#)
- [Reposition an AP on a Map, on page 151](#)
- [Reposition a Sensor on a Map, on page 156](#)


To configure other floor map elements or overlays, you need to use the 2D map. For details, see [2D Floor Map Devices and Overlay Objects, on page 145](#).

Clone an AP

You can duplicate an AP with its configuration by cloning it.

Before you begin

You must have actual APs to clone.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
 - Step 2** From the left hierarchy tree, choose a floor.
 - Step 3** In the map toolbar, click **3D**.
 - Step 4** In the map toolbar, click the simulation icon .
 - Step 5** In the map toolbar, click **Add/Edit**.

Step 6 On the map, click an AP.

Step 7 In the **AP Details** slide-in pane, click **Clone**.

A duplicate AP is created and displayed below the original AP. Its name is appended with **-1**. If you keep cloning the same AP, the name continues to be incrementally appended. For example, the first clone for **a-floor1-ap01** is named **a-floor1-ap01-1**, the second clone for the same AP is named **a-floor1-ap01-2**, and so on.

Step 8 On the map, right-click the cloned AP and choose **Move**.

Step 9 Drag and drop the AP to its new position.

Step 10 Click **Save**.

View a 3D Wireless Map

Use this procedure to view a 3D wireless map.

Step 1 Click the menu icon (☰) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **3D**.

The 3D wireless map opens.

Note A 3D heatmap is delimited by its coverage area, which is the full floor width and length, by default. To specify a polygon for the heatmap boundaries, edit the **Coverage Area** field value in the 2D map view. However, these boundaries don't apply to the 2D map view because the full floor width and length are used for the 2D map view.

Step 4 To display specific details about devices, hover your cursor over the device icon. Information about the device is displayed in a dialog box.

Note If the *Assurance - Base* package is installed, a link to the **Device 360** window is also displayed in the dialog box.

Step 5 To view the heatmap for one or more APs, select and deselect the APs using one of the following methods:

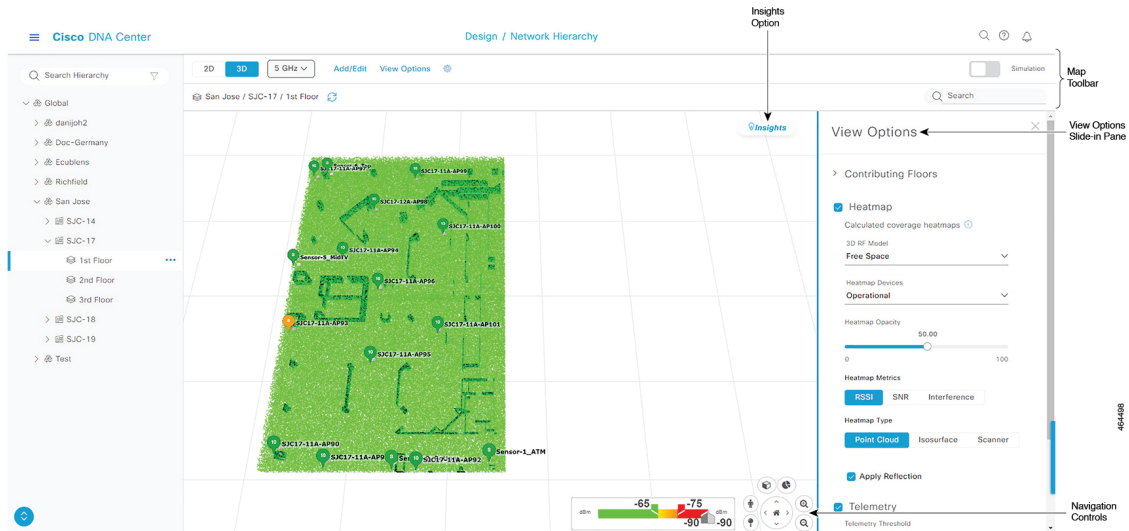
- To select a single AP, click the AP.
- To select multiple APs, press the **Shift** key while clicking each AP, and then release the **Shift** key.
- To deselect a single AP, click the AP.

Note If no APs are selected, the heatmap includes all APs.

- To deselect all APs, press the **ESC** key or double-click an area of the map that doesn't have any APs.

Step 6 Use the tools and options shown in the following figure to gain insights about your wireless network.

Figure 11: 3D Wireless Map Showing Tools and Options







- **Toolbar:** Above the map, use the toolbar options to control what's displayed on the heatmap. For details, see [3D Wireless Map Toolbar, on page 175](#).
- **Insights:** In the top-right corner of the map, click **Insights** to view and understand potential issues in your wireless network. For details, see [Gain Insights from a 3D Wireless Map, on page 186](#).
- **View Options:** In the slide-in pane, use the view options to control the heatmap display. You can manipulate elements, such as which floors that are displayed, heatmap coverage and metrics, telemetry thresholds, devices and clients, overlay objects, and the depiction of a floor and sky. For details, see [3D Map View Options, on page 176](#)
- **Navigation Controls:** In the bottom-right corner of the map, use the map navigation controls to view the heatmap from various perspectives. For details, see [3D Map Navigation Controls, on page 179](#).

3D Wireless Map Toolbar


To access the 3D map, click the menu icon (☰) and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, choose a floor, and in the map toolbar, click **3D**.

The map toolbar consists of two bars and is located above the map. Use the map toolbar for the following actions and settings:

Item	Description
	Click 3D to view the wireless map in 3D or click 2D to view it in 2D.
	Click the Wi-Fi band down arrow and choose a Wi-Fi band.

Item	Description
Add/Edit	<p>Click Add/Edit to add planned APs by cloning the existing APs or planned APs. For details, see Clone an AP, on page 173.</p> <p>Note The option to add operational APs from the inventory is not available in 3D. To add operational APs, click Add/Edit in the 2D map toolbar.</p>
View Options	<p>Open the 3D Floormap slide-in pane to display the contributing floors, KPIs, telemetry, device and client information, and floor element settings. For details, see 3D Map View Options, on page 176.</p>
	<p>Hover your cursor over the gear icon and click Insights Configuration to customize the conditions for insights. For details, see Gain Insights from a 3D Wireless Map, on page 186.</p>
Simulation	<p>Click the Simulation toggle button to view the map in simulation mode. The default view is operation mode. For details, see Create Simulations for 3D Wireless Maps, on page 188.</p> <p>Note Simulation mode is available only in 3D maps, not in 2D maps.</p>
 Area or Site / Building / Floor	<p>Full Hierarchy Path: Displays the full navigational path of the floor, including its associated building and site. Click the down arrow to navigate to a different floor.</p>
	<p>Click the refresh icon to update the device and map data. To the left of the icon is the timestamp for the last refresh.</p>
 Search	<p>Use the Search field to find specific floor map elements such as APs, sensors, clients, and so on. The results of your search are listed below the Search field.</p> <p>When you hover your cursor over an element in the list, an indicator points to the element on the map. If the element is outside the field of view, the indicator is displayed as a broken red line. Reorient the map to see the element.</p>

3D Map View Options

To access the 3D map, click the menu icon () and choose **Design > Network Hierarchy**. From the left hierarchy tree, choose a floor, and in the map toolbar, click **3D > View Options**.

The **View Options** slide-in pane opens. Expand the categories to view the settings:

- **Contributing Floors:** Expand this option to include more floors in the heatmap computation. When including a floor, you can choose to add its APs in the heatmap computation and display its APs and floor geometry. Click **Apply** to generate the heatmap with your settings.

Figure 12: 3D Map of Multiple Floors



Item	Description
Compute APs	Check this check box to include a floor's APs when computing the heatmap.
Display APs	Check this check box to display a floor's APs in the heatmap.
Display Geometry	Check this check box to display a floor's physical attributes in the heatmap.

- **Heatmap:** Check this check box to display the heatmap and to configure the settings in the following table:

Item	Description
3D RF Model	Use this drop-down list to choose the RF model. The RF model determines how RF is calculated based on the floor geometry. Available models include drywall offices, cubes and walled offices, free space, outdoor open space, and indoor high ceiling. Note We recommend that you choose Free Space if you manually placed the walls or imported them from a CAD file or Ekahau project. If you didn't manually place the walls, use an RF model other than Free Space .
Heatmap Devices	Use this drop-down list to choose whether to display operational devices, operational and planned devices, or only planned devices on the heatmap.
Heatmap Opacity	Use this slider to customize the opacity or transparency of the heatmap.

Item	Description
Heatmap Metrics	<p>Choose the type of metrics to display on the heatmap:</p> <ul style="list-style-type: none"> • RSSI: Displays the Received Signal Strength Indicator (RSSI) values. • SNR: Displays the signal-to-noise ratio (SNR) values. • Interference: Displays the SNR that is caused by co-channel interference (CCI) or adjacent channel interference. • Leakage: Displays signal leakage between floors. For this option to be available, you must compute the heatmap with two or more contributing floors.
Heatmap Type	<p>Choose the heatmap type:</p> <ul style="list-style-type: none"> • Point Cloud: Provides a collection of data points in space. Each data point has x, y, and z coordinates. • Isosurface: Represents the RSSI with isolines or lines of a contiguous value. • Scanner: Displays the RSSI for a specific elevation.
Apply Reflection	<p>Check this check box to show signal reflection, which can be caused when a signal bounces off materials such as glass, whiteboards, and plastic.</p>
Telemetry	<p>Use this toggle button to enable or disable telemetry.</p> <p>When telemetry is enabled, click a sensor or AP to view its telemetry:</p> <ul style="list-style-type: none"> • The telemetry for a sensor displays the predicted and measured RSSI values between a sensor AP and other APs. • The telemetry for an AP displays the predicted and measured RSSI values between neighbor APs.

- **Telemetry**: Check this check box and use the **Telemetry Threshold** slider to set the threshold for telemetry sources to be displayed on the heatmap.

Telemetry sources with predicted values that do not meet the threshold are faded.

- **Devices and Clients**: Click this option to configure the settings in the following table:

Item	Description
APs	Check this check box to display APs on the map.
Planned APs	Check this check box to display planned APs on the map.
Sensors	Check this check box to display sensors on the map.

Item	Description
Clients	<p>Check this check box to display clients on the map. Additionally, you can do the following:</p> <ul style="list-style-type: none"> • Display clients in their default blue color (None) or by their RSSI, SNR, or Health Score. For RSSI, SNR, and Health Score, clients are colored blue, yellow, or red, depending on their current condition. • Use the slider to change the size of the ball that represents a client on the map.


- **Overlay Objects:** Click this option to configure the settings in the following table:

Item	Description
Geometry	Check this check box to display the floor geometry.
Height	Use this slider to set the height of walls on the heatmap.

- **Map:** Click this option to configure the settings in the following table:


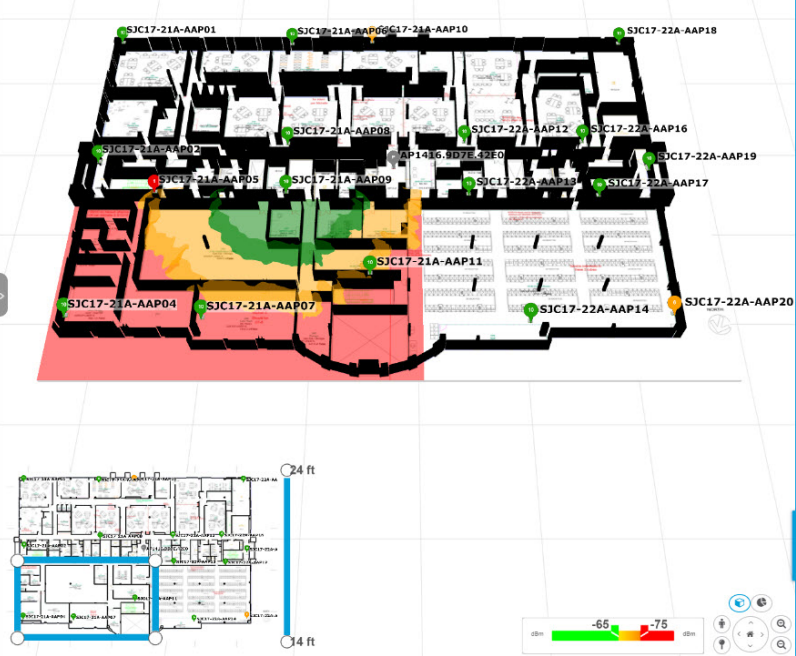
Item	Description
Sky	Check this check box to display the sky in the heatmap.
Floor	Check this check box to display the floor in the heatmap.




3D Map Navigation Controls



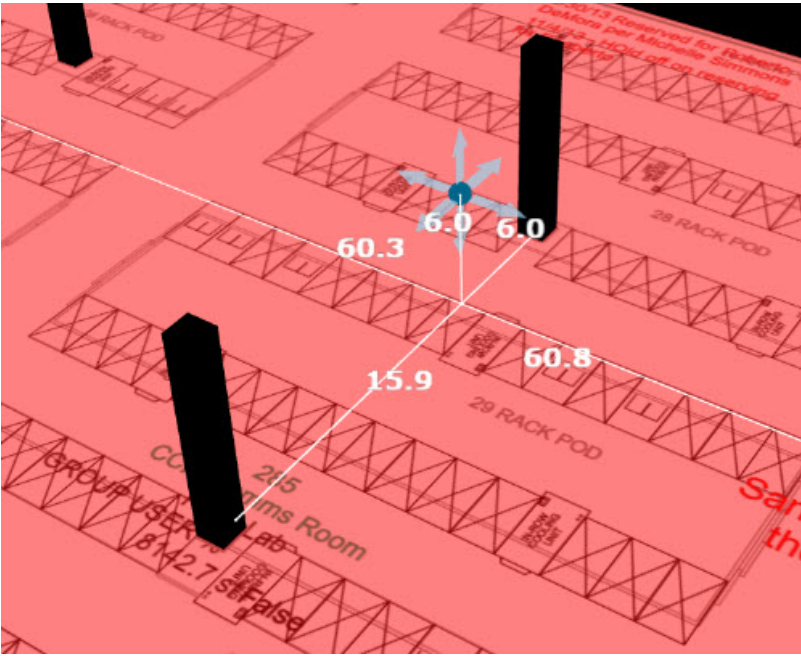

To access the 2D map, click the menu icon () and choose **Design** > **Network Hierarchy**. From the left hierarchy tree, choose a floor, and in the map toolbar, click **3D**.



The 3D map navigation controls are located at the bottom-right corner of the map. For details about the map, see [View a 3D Wireless Map, on page 174](#).

Use the map navigation controls at the bottom-right corner of the map to control the map view.

Map Navigation Control	Description
	<p>Use clip box: Click this icon to crop the heatmap using a box shape. Use the clipper at the bottom-left corner of the map to specify the crop:</p> <ul style="list-style-type: none"> • Click and drag one of the anchor points to change the size of the crop. • Click and drag one of the anchor points on the right vertical slider to specify the height range of the crop. <p>Figure 13: Clip Box</p> 

Map Navigation Control	Description
	<p>Use clip planes: Click this icon to crop the heatmap using a donut shape. Use the clipper at the bottom-left corner of the map to specify the crop:</p> <ul style="list-style-type: none"> • Click and drag the anchor point in the center of the donut to reposition the donut. • Click and drag the two outer anchor points to change the shape of the crop. <p>Figure 14: Clip Planes in Use</p> 
	<p>First Person View: Click this icon to switch between first-person view and third-person view.</p> <p>The blue sphere indicates your position on the map. As you move throughout the map, your field of view changes. You can use the mini map at the lower-left corner to get an idea of your field of view and orientation.</p> <p>Note If you have more than one floor selected for display, the First Person View automatically positions you on the current floor.</p> <p>For details, such as the controls for view, see Use First-Person and Third-Person Views for 3D Wireless Maps, on page 183.</p>

Map Navigation Control	Description
	<p>Third Person View: Click this icon to switch between first person view and third person view. You can also drag and drop the icon on the map where you want to be positioned.</p> <p>The blue sphere indicates your position on the map. As you move throughout the map, your field of view changes. You can use the mini map at the lower-left corner to get an idea of your field of view and orientation.</p> <p>For details, such as the controls for view, see Use First-Person and Third-Person Views for 3D Wireless Maps, on page 183.</p>
	<p>Place a pin: Click this icon to view a predicted measurement (x, y, and z coordinates) of a specific point on the floor map. By placing a pin, you can view the measurements of the distance from the pin to the end of the yard stick. As you zoom in or zoom out, the position of the measurements is adjusted to stay in your view. Drag and drop the pin to change its position, as follows:</p> <ul style="list-style-type: none"> • To move the pin horizontally: Click the horizontal arrows and drag the pin left, right, forward, or backward. The selected arrows and yard stick are highlighted while active. • To move the pin vertically: Click the vertical arrows and drag the pin up or down. The selected arrows and yard stick are highlighted while active. <p>For a video demonstration, click here.</p> <p>Figure 15: Adjusting a Pin</p> 
	<p>Zoom In: Click this icon to enlarge the view. Alternatively, you can use your mouse wheel to zoom in.</p>

Map Navigation Control	Description
	Zoom Out: Click this icon to reduce the size of the image and to increase your field of view. Alternatively, you can use the scroll wheel on your mouse to zoom out.
	Map Rotation and Default Map View: Click the directional arrows to change the camera angle. Click the Return Home icon to reset the map to the default view.



Use First-Person and Third-Person Views for 3D Wireless Maps

You can use the first-person and third-person views to gain different perspectives of your wireless network.

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

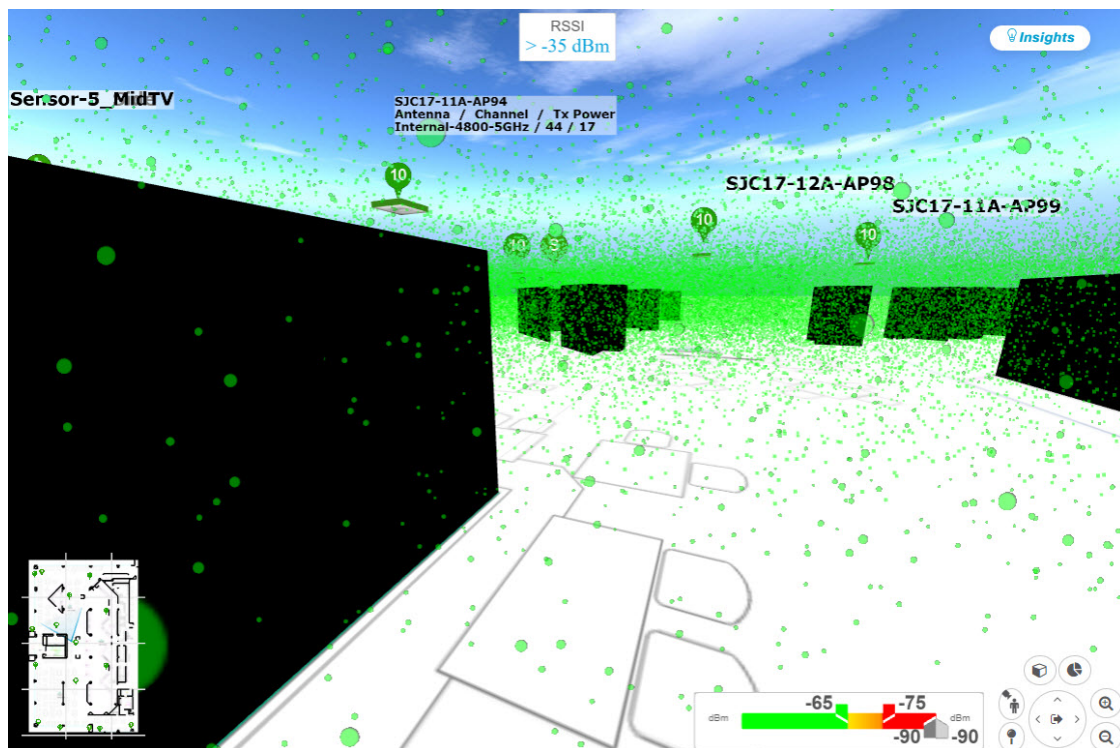
Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **3D**.

Step 4 To use the first-person view, click the first-person view icon  in the map navigation controls. Optionally, you can drag and drop the person icon  to a specific location on the map.

The map view changes to the first-person view.

Figure 16: First-Person View



Step 5 You can control the first-person view by doing the following:

Action	Controls
Move forward/backward and right/left.	Use the W , A , S , and D keys or arrow keys.
Change the camera angle.	Click and hold the left mouse button on the map and move the mouse wheel.
Raise the altitude of the camera angle.	Hold the Spacebar .
Lower the altitude of the camera angle.	Hold Shift + Spacebar .


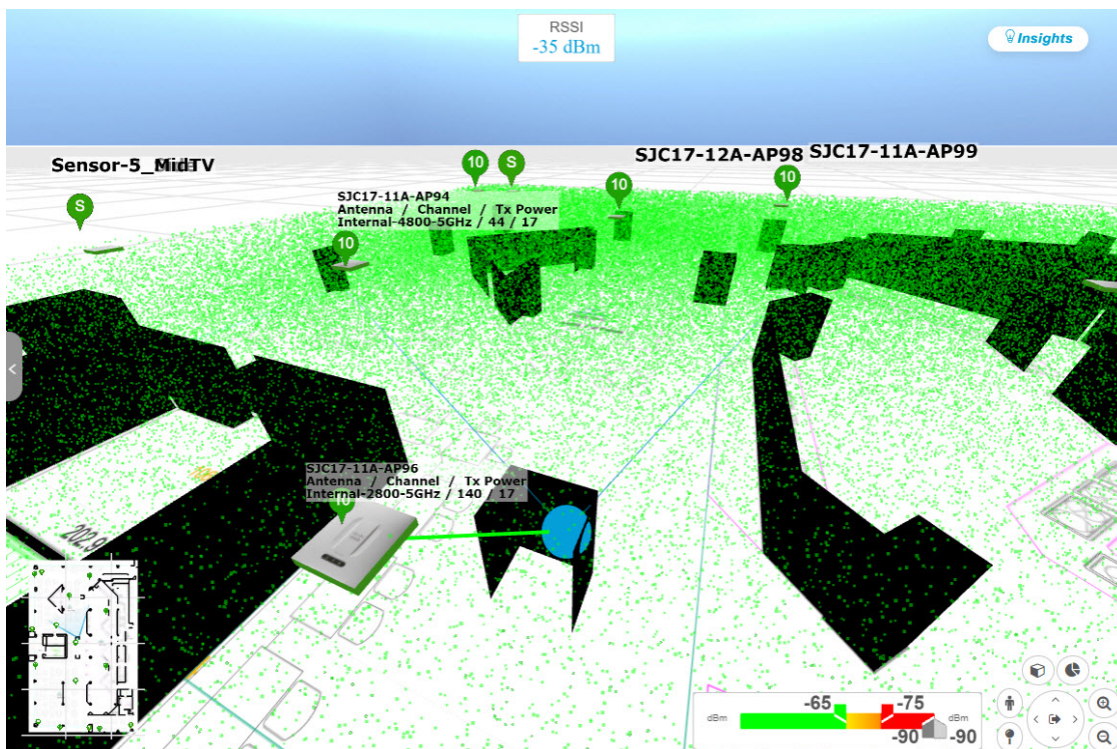
Step 6 To use the third-person view, click the third-person view icon  from the map navigation controls. The map view changes to the third-person view.

Figure 17: Third-Person View



Step 7 You can control the third-person view by doing the following:

Action	Controls
Move forward/backward and right/left.	Use the W , A , S , and D keys or arrow keys.
Change the camera angle.	Click and drag on the map.
Raise the altitude of the camera angle.	Hold the Spacebar .

Action	Controls
Lower the altitude of the camera angle.	Hold Shift + Spacebar .

Step 8 To return to the default view, click the return home icon



Display Details About APs and Clients

If you have a location service, such as Cisco Spaces or Cisco Connected Mobile Experiences (CMX), installed on Cisco DNA Center you can view the locations of clients on a floor. Clients are identified as a small blue ball (●) on the map.

SUMMARY STEPS

1. Click the menu icon and choose **Design > Network Hierarchy**.
2. From the left hierarchy tree, choose a floor.
3. From the map toolbar, click **3D**.
4. To display details about an AP, click it.
5. To display information about a client, hover your cursor over the ball (client).
6. To display the client in a color that corresponds to its RSSI, SNR, or health score, do the following:
7. To resize the ball, use the **Ball Size** slider in the **View Options** pane. This feature helps you view clients in cases where there are many clients or only a few. For example, in cases where there are many clients, you may want to make the ball smaller, and in cases where there are only a few clients, you may want to make the ball larger.

DETAILED STEPS

Step 1 Click the menu icon and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 From the map toolbar, click **3D**.

Note A 3D heatmap is delimited by its coverage area, which is the full floor width and length, by default. To specify a polygon for the heatmap boundaries, you need to edit the **Coverage Area** field value in the 2D map view. However, these boundaries do not apply to the 2D map view, as the full floor width and length is used for the 2D map view.

Step 4 To display details about an AP, click it.

Step 5 To display information about a client, hover your cursor over the ball (client).

A line is drawn between the client and its associated AP. A dialog box is displayed with information, such as the client's IPv4 address, IPv6 IP address, RSSI value, and so on. To open the **Client 360** page, click the **Client 360** link in the dialog box.

Step 6 To display the client in a color that corresponds to its RSSI, SNR, or health score, do the following:

- a) Click **View Options > Devices and Clients**.

- b) Click the **Clients** check box.
- c) Under the **Clients** check box, click **None** (default blue color), **RSSI**, **SNR**, or **Health Score**.

Step 7 To resize the ball, use the **Ball Size** slider in the **View Options** pane. This feature helps you view clients in cases where there are many clients or only a few. For example, in cases where there are many clients, you may want to make the ball smaller, and in cases where there are only a few clients, you may want to make the ball larger.

Gain Insights from a 3D Wireless Map

Cisco DNA Center actively monitors the network performance of 3D wireless maps and provides insights into areas where service-level agreements (SLA) are not being met.

Step 1 Click the menu icon () and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **3D**.

Step 4 At the top-right corner of the map, click **Insights**.


The **Insights** area opens and displays information about the coverage areas that don't meet a specific KPI threshold, for example, RSSI is ≥ -70 dBm.

Figure 18: Insights Area



Step 5 In the **Insights** area, you can do any of the following actions:

Item	Details
View coverage gaps	Click this link to display the wireless coverage area. Red areas show where the SLA is not being met. Green areas show where it's being met.
Optimizer	Click this link to have Cisco DNA Center analyze the wireless coverage area. You can indicate the maximum number of APs that you are willing to move and add, and Cisco DNA Center computes a configuration where the wireless coverage is maximized. For more information, see Run the Wireless Coverage Optimizer, on page 187 .
Mute This Insight	Click this button to exclude an insight from displaying in the Insights dialog box. Muted insights appear at the bottom of the list in the All Insights slide-in pane.

Item	Details
View All Insights	<p>Click this button to display all active and muted insights.</p> <p>For each insight, you can click Mute or Unmute to exclude or include its display in the Insights dialog box.</p> <p>Click Edit Configuration to customize the insight KPI settings.</p> <p>Another way to customize insight KPI settings is from the map toolbar. Hover your cursor over the gear icon  in the map toolbar and choose Insights Configurations.</p>

Run the Wireless Coverage Optimizer

For wireless areas that aren't meeting their SLA, the optimizer takes your input of the maximum number of APs that you are prepared to move and add, and computes a configuration where the wireless coverage is maximized.

This procedure shows you how to run the wireless coverage optimizer.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose a floor.
- Step 3** In the map toolbar, click **3D**.
- Step 4** At the top-right corner of the map, click **Insights**.
- The **Insights** area opens and displays information about the coverage areas that don't meet a specific KPI threshold, for example, RSSI is ≥ -70 dBm.
- Step 5** (Optional) To display the wireless coverage area, click **View**.
- Red areas show where the SLA is not being met. Green areas show where the SLA is being met.
- Step 6** (Optional) If there are specific APs that you don't want the optimizer to move, you can right-click them and choose **Lock** to lock their position. To remove the lock, right-click the AP and choose **Unlock**.
- Step 7** Click **Optimizer**.
- Step 8** In the **Coverage Optimizer** dialog box, enter the maximum number of APs that you are prepared to move and add. If you don't want to move or add APs, leave the corresponding field blank or enter **0**.
- Step 9** Click **Run Optimizer**.
- If needed, you can manually move any of the APs to other locations.
- Step 10** When the analysis is complete, click **View Results**.
- Cisco DNA Center displays a proposed layout that increases the wireless coverage to maximize the SLA. If the optimizer recommends moving an AP, the new layout displays a blue line to the recommended new location. Any new APs that have been added to the layout are displayed as blue markers (📍).
- Step 11** To save the new layout as a simulation, click **Save as a plan**. To exit without saving, click the **x** at the top-right corner of the map.

Later, if you implement the recommended changes to your physical wireless network, you can save the simulation as an operational map. For information, see [Create Simulations for 3D Wireless Maps, on page 188](#).

Create Simulations for 3D Wireless Maps

You can create simulations for 3D wireless maps.



Note Simulation mode is available only in 3D maps, not in 2D maps.

Simulations allow you to change device configurations without actually implementing them. You can create multiple simulations and load them at any time.

Step 1 Click the menu icon (\equiv) and choose **Design > Network Hierarchy**.

Step 2 From the left hierarchy tree, choose a floor.

Step 3 In the map toolbar, click **3D**.

Step 4 In the map toolbar, click the **Simulation** toggle button.

The 3D wireless map enters the simulation mode, which is indicated by the color of the lower map toolbar changing to light blue.

Step 5 In the map toolbar, click **Add/Edit**.

In the simulation mode, only particular attributes are editable for previewing the impact of changes on the heatmap.

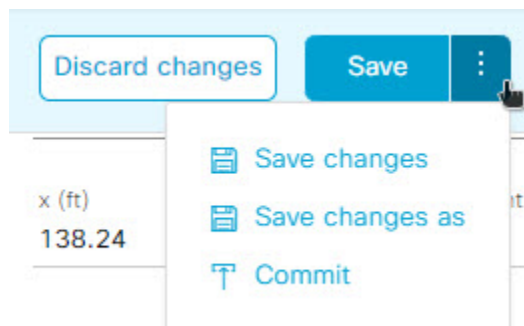
Step 6 Make the changes to the devices, as needed:

- **APs:** You can change the model, channel, and transmission power.
- **PAPs:** You can change the channel and transmission power.

a) Click **Apply**.

Step 7 In the map toolbar, hover your cursor over the vertical ellipsis and choose **Save changes as**.

Figure 19: Saving as a Simulation



Note Choosing **Save changes** saves your changes to the Operation mode.
Choosing **Commit** saves your changes to the production devices.

Step 8 In the **Save Simulation** dialog box, enter a name for the simulation and click **Save**.

Step 9 To load a simulation, click the **Simulation** toggle button and, from the **Select Simulation** drop-down list, choose a simulation. If you have no saved simulations, **None available** is displayed.



CHAPTER 9

Configure Network Settings

- [Network Settings Overview](#), on page 191
- [Add Cisco ISE or Other AAA Servers](#), on page 192
- [Configure Global Network Servers](#), on page 193
- [Global Device Credentials Overview](#), on page 194
- [Configure IP Address Pools](#), on page 202
- [Configure Service Provider Profiles](#), on page 207
- [Configure Global Wireless Settings](#), on page 207
- [Configure a Certificate Revocation Check](#), on page 273

Network Settings Overview

You can create network settings that become the default for your entire network. There are two primary areas from which you can define the settings within your network:

- **Global settings:** Settings defined here affect your entire network and include settings for servers such as DHCP, DNS, AAA, NTP, and so on; IP address pools; Device Credential profiles; Telemetry settings such as Syslog, Traps, and NetFlow.
- **Site settings:** Settings defined here override global settings and can include settings for servers, IP address pools, and device credential profiles.



Note Changes in network settings that are being used by the active fabric are not supported. These network settings include site hierarchy, renaming IP pools, and several other features.



Note Certain network settings can be configured on devices automatically using the Device Controllability feature. When Cisco DNA Center configures or updates devices, the transactions are captured in the Cisco DNA Center audit logs. You can use the audit logs to help you track changes and troubleshoot issues.

You can define the following global network settings by choosing **Design > Network Settings** and clicking the appropriate tab.

- Network servers, such as AAA, DHCP, and DNS: For more information, see [Configure Global Network Servers, on page 193](#).
- Device credentials, such as CLI, SNMP, and HTTP(S): For more information, see [Configure Global CLI Credentials, on page 194](#), [Configure Global SNMPv2c Credentials, on page 195](#), [Configure Global SNMPv3 Credentials, on page 195](#), and [Configure Global HTTPS Credentials, on page 197](#).
- IP address pools: For more information, see [Configure IP Address Pools, on page 202](#).
- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles: For more information, see [Configure Global Wireless Settings, on page 207](#).
- Configure global telemetry settings, such as syslog, SNMP, and NetFlow Collector servers using telemetry.

Add Cisco ISE or Other AAA Servers

You can define Cisco Identity Services Engine (ISE) servers or other, similar AAA servers for network, client, and endpoint authentication at the site or global level. For network authentication, RADIUS and TACACS protocols are supported. For client and endpoint authentication, only RADIUS is supported. Only one Cisco ISE is supported per Cisco DNA Center.

You can configure the source interface under the RADIUS or TACACS server group to support multi-ISE configuration, wherein each Cisco ISE cluster has its own server group. The source interface used for RADIUS and TACACS servers is determined in the following way:

- If the device has a Loopback0 interface configured, Loopback0 is configured as the source interface.
- Otherwise, the interface that Cisco DNA Center uses as the management IP is configured as the source interface.

After you configure a Cisco ISE server for a site, the devices that are assigned to the site are automatically updated on the corresponding Cisco ISE server with a /32 mask. Subsequently, any changes to those devices in Cisco ISE are sent automatically to Cisco DNA Center.

For FIPS mode of deployment, the shared secret consists of shared secret, keywrap, and message authenticator code key.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Network**.
- Step 2** Click **Add Servers** to add a AAA server.
- Step 3** In the **Add Servers** window, check the **AAA** check box, and click **OK**.
- Step 4** Set the AAA server for network users, client/endpoint users, or both.
- Step 5** Check the **Network** and/or **Client/Endpoint** check boxes and configure servers and protocols for the AAA server.
- Step 6** Choose the **Servers** for authentication and authorization: **ISE** or **AAA**.

- If you choose **ISE**, configure the following:
 - From the **Network** drop-down list, choose the IP address of the Cisco ISE server. The **Network** drop-down list contains all the IP addresses of the Cisco ISE servers that are registered in **System Settings** on the Cisco DNA Center home page. Selecting a Cisco ISE IP populates the primary and additional IP address drop-down lists with Policy Service Node (PSN) IP addresses for the selected Cisco ISE. You can either enter an IP address

for the AAA server or choose the PSN IP address from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists.

- Choose the **Protocol**: **RADIUS** or **TACACS**.

Note AAA settings for a physical and managed site for a particular wireless controller must match, or provisioning fails.

- If you choose **AAA**, configure the following:

- Enter an IP address for the AAA server or choose the IP addresses from the **IP Address (Primary)** and **IP Address (Additional)** drop-down lists. These drop-down lists contain the non-Cisco ISE AAA servers registered in the **System Settings**.

Ensure that the AAA server IP address is not part of an existing Cisco ISE cluster.

Note If you switch the server type from ISE (with TACACS) to AAA with TACACS, TACACS will be disabled on the Cisco ISE server because it is no longer used for authentication.

Step 7 Click **Save**.

Configure Global Network Servers

You can define the global network servers that become the default for your entire network.



Note You can override the global network settings on a site by the defining site-specific settings.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > Network**.

Step 2 In the **DHCP Server** field, enter the IP address of a DHCP server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DHCP server in order to create IP address pools.

Step 3 In the **DNS Server** field, enter the domain name of a DNS server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DNS server in order to create IP address pools.

Step 4 Click **Save**.

Global Device Credentials Overview

"Global device credentials" refers to the common CLI, SNMP, and HTTPS credentials that Cisco DNA Center uses to discover and collect information about the devices in your network. Cisco DNA Center uses global credentials to authenticate and access the devices in a network that share these configured device credentials. You can add, edit, and delete global device credentials. You can also associate credentials to the Global site or a specific site.

Configure Global CLI Credentials

You can configure and save up to 10 global CLI credentials.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Device Credentials**.
- Step 2** From the left hierarchy tree, choose **Global**.
- Step 3** In the **CLI Credentials** area, click **Add**.
- Step 4** Enter information in the following fields:

Table 28: CLI Credentials

Field	Description
Name/Description	Name or phrase that describes the CLI credentials.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	<p>Password that is used to log in to the CLI of the devices in your network.</p> <p>For security reasons, re-enter the password as confirmation.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Enable Password	<p>Password used to move to a higher privilege level in the CLI. Configure this password only if your network devices require it.</p> <p>For security reasons, re-enter the enable password.</p> <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

- Step 5** Click **Save**.
To apply the credential to a site, choose the site from the left hierarchy tree, select the button next to the credential, then click **Save**.
- Step 6** If you are changing existing credentials, choose whether you want to update the credentials now or schedule it for later.

Configure Global SNMPv2c Credentials

You can configure global SNMPv2c credentials to monitor and manage your network devices.



Note Cisco DNA Center does not support SNMPv2c device credentials when FIPS mode is enabled. You must specify SNMPv3 credentials instead.

Before you begin

You must have the SNMP information for your network.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Device Credentials**.
- Step 2** From the left hierarchy tree, choose **Global**.
- Step 3** In the **SNMP Credentials** area, click **Add**.
- Step 4** For the Type, click **SNMP v2c** and enter the following information:

Table 29: SNMPv2c Credentials

Field	Description
Read	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Read Community: Read-only community string password used only to view SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>
Write	<ul style="list-style-type: none"> • Name/Description: Name or description of the SNMPv2c settings that you are adding. • Write Community: Write community string used to make changes to the SNMP information on the device. <p>Note Passwords are encrypted for security reasons and are not displayed in the configuration.</p>

- Step 5** Click **Save**.
- Step 6** If you are changing existing credentials, choose whether you want to update the credentials **Now** or schedule it for later.

Configure Global SNMPv3 Credentials

You can configure global SNMPv3 credentials to monitor and manage your network devices.

Before you begin

You must have your network's SNMP information.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Device Credentials**.
- Step 2** From the left hierarchy tree, choose **Global**.
- Step 3** In the **SNMP Credentials** area, click **Add**.
- Step 4** For the Type, click **SNMP v3** and enter the following information:

Table 30: SNMPv3 Credentials

Field	Description
Name/Description	Name or description of the SNMPv3 settings that you are adding.
Username	Name associated with the SNMPv3 settings.
Mode	Security level that an SNMP message requires. Choose one of the following modes: <ul style="list-style-type: none"> • noAuthNoPriv: Does not provide authentication or encryption. • AuthNoPriv: Provides authentication, but does not provide encryption. • AuthPriv: Provides both authentication and encryption.
Auth Type	Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types: <ul style="list-style-type: none"> • SHA: Authentication based on HMAC-SHA • MD5: Authentication based on HMAC-MD5
Auth Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. <p>Note</p> <ul style="list-style-type: none"> • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select AuthPriv as the authentication mode.) Choose one of the following privacy types: <ul style="list-style-type: none"> • DES: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard. • AES128: CBC mode AES for encryption. • None: No privacy.

Field	Description
Privacy Password	<p>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least eight characters long.</p> <p>Note</p> <ul style="list-style-type: none"> Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. Passwords are encrypted for security reasons and are not displayed in the configuration.

Step 5 Click **Save**.

Step 6 If you are changing existing credentials, you are prompted to update the new credentials on devices now or schedule the update for a later time.

- To update the new credentials now, click the **Now** radio button and click **Apply**.
- To schedule the update for a later time, click the **Later** radio button, define the date and time of the update and click **Apply**.

Note Use the **Time Zone** check box to indicate whether you want the update to happen according to the site time zone or according to a specified time zone.

Configure Global HTTPS Credentials

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > Device Credentials**.

Step 2 From the left hierarchy tree, choose **Global**.

Step 3 In the **HTTPS Credentials** area, click **Add**.

Step 4 Enter the following information:

Table 31: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write .

Field	Description
Read	<p>You can configure up to 10 HTTPS read credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>
Write	<p>You can configure up to 10 HTTPS write credentials:</p> <ul style="list-style-type: none"> • Name/Description: Name or description of the HTTPS credentials that you are adding. • Username: Name used to authenticate the HTTPS connection. • Password: Password used to authenticate the HTTPS connection. Passwords are encrypted for security and are not displayed in the configuration. • Port: Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS). <p>The password must contain between 7 and 128 characters, including at least one of the following:</p> <ul style="list-style-type: none"> • Lowercase letter (a to z) • Uppercase letter (A to Z) • Number (0 to 9) • Special character: # _ * ? – <p>The password cannot contain spaces or angle brackets (<>). Note that some Cisco IOS XE devices do not allow a question mark (?).</p>

Step 5 Click **Save**.

Step 6 If you are changing existing credentials, choose whether you want to update the credentials **Now** or schedule it for later.

Guidelines for Editing Global Device Credentials

The following are guidelines and limitations for editing existing global device credentials:

- Cisco DNA Center uses the following process when you edit, save, and then apply a global device credential:
 1. Cisco DNA Center pushes the credential to the device that has local authentication. With local authentication, credential changes are applied and Cisco DNA Center manages the devices using these credentials.

(Cisco DNA Center does not push CLI credential changes to a device that is under a site with an inherited or configured AAA server. With AAA authentication, credential changes are not applied. Cisco DNA Center manages the devices using these credentials only if the same credentials exist on the AAA server.)
 2. After successfully pushing the credential to the device, Cisco DNA Center confirms it can reach the device using the new credential.



Note If this step fails, Inventory uses the old credentials to manage the device even though Cisco DNA Center pushed the new credentials to the device. In this case, the **Provision > Inventory** window might indicate that the device is Unmanaged if you updated an existing credential.

3. After successfully reaching the device using the new credential, the Cisco DNA Center Inventory starts managing the device using the new credential.
- Sites can contain devices that use SNMPv2c and SNMPv3 credentials. When you edit and save global SNMPv2c or SNMPv3 credentials, Cisco DNA Center pushes those changes to devices and enables that credential. For example, if you have a device that uses SNMPv2c, but you edit and save the SNMPv3 global credential, Cisco DNA Center pushes the new SNMPv3 credential to all devices in the associated site and enables it, meaning that all devices will be managed using SNMPv3, even the devices that previously had SNMPv2c enabled.
 - To avoid any possible disruptions, modify the **User Name** when you edit CLI credentials. This creates a new CLI credential and leaves any existing CLI credentials unchanged.

Edit Global Device Credentials

You can edit and save global device credentials without Cisco DNA Center applying those credential changes until you're ready. When you decide to apply the changes, Cisco DNA Center searches all sites that reference the device credential you changed and pushes the change to all the devices.

You can update or create new global device credentials, but Cisco DNA Center never removes any credentials from devices.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > Device Credentials**.

Step 2 From the left hierarchy tree, choose **Global**.

Step 3 Click **Manage Credentials**, check the check box for the device credential that you want to change, and choose **Actions > Edit**.

Step 4 In the **Edit Credentials** dialog box, make the required changes, and click **Save**.

Note The CLI password credentials support only *ASCII-printable characters* (character code 32-127; see https://en.wikipedia.org/wiki/ASCII#Printable_characters).

Step 5 In the credential tile, click **Apply**.

Step 6 In the **Apply Credentials** dialog box, choose whether you want to update the credentials **Now** or schedule it for later.

Step 7 To view the status of the credential change, choose **Provision > Network Devices > Inventory**.

The **Credential Status** column displays one of the following statuses:

- Success: Cisco DNA Center successfully applied the credential change.
- Failed: Cisco DNA Center was unable to apply the credential change. Hover over the icon to display additional information about which credential change failed and why.
- Not Applicable: The credential is not applicable to the device type.

If you edited and saved more than one credential (for example, CLI, SNMP, and HTTPS), the **Credential Status** column displays **Failed** if Cisco DNA Center was unable to apply *any* of the credentials. Hover the cursor over the icon to display additional information about which credential change failed.

Associate Device Credentials to Sites

The sites you create under the Global site can inherit the global device credentials, or you can create different device credentials specific for a site.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > Device Credentials**.

Step 2 From the left hierarchy tree, choose the required site.

Step 3 Click **Manage Credentials**.

Step 4 Select the credentials that you want to associate with the selected site and then click **Assign**.

A success message is displayed at the bottom of the screen indicating the device credential was successfully associated with the site.

Manage Device Credentials

The Manage Credentials workflow allows you to create, edit, assign, and apply credentials to devices.

Credentials are assigned to the **Global** site or to the sites, buildings, or floors that you choose. If you assign credentials at the global level, all the sites, buildings, and floors inherit the settings from the global level.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > Device Credentials**.

Step 2 From the left hierarchy tree, choose either **Global** or the required area, building, or floor.

Step 3 Click **Manage Credentials**.

The **Manage Credentials** window opens.

Step 4 From the **Add** drop-down list, choose a type of credential, for example, CLI, HTTP(S) Read, SNMPv3, and so on.

Step 5 In the **Add New Credentials** window, do the following:

- a. Enter information in the required fields.
- b. Check the **Assign credential to site** check box.

Note If the box is not checked, the credential will get created but not assigned to any site.

- c. Click **Save**.

The newly created credential is displayed in the **Manage Credentials** window.

Step 6 Choose the credential that you want to assign and click **Assign**.

Step 7 To apply the credentials, do any one of the following:

- To apply a credential across the entire site hierarchy, go to **Manage Credentials**, hover your cursor over the **Actions** menu for the required credential, and choose **Apply**.
- To apply a credential only to a specific site, choose the desired site in the left hierarchy pane and click **Assign** on the card corresponding to that credential.

Step 8 In the **Apply Credentials** dialog box, choose whether you want to update the credentials **Now** or schedule it for later.

The credentials are applied to all the applicable sites.

You can reschedule any apply credentials task that has not yet started.

Step 9 To view the status of your task, do any one of the following:

- In the **Device Credentials** window, click the refresh icon at the top-right corner. Hover your cursor over the icon next to the heading in the credential card.
- Choose **Provision > Inventory**. The **Credential Status** column shows the status.
- Choose **Activities > Audit Log**.

Step 10 To edit the credentials, do the following:

- a. Click the edit icon next to the corresponding credential.

Alternatively, in the **Manage Credentials** window, hover your cursor over the ellipsis icon next to the credential name and click **Edit**.

- b. In the **Edit Information** window, click **OK**.
- c. In the **Edit Credentials** window, make the required changes.
- d. Click **Save**.

Step 11 To reschedule the **Start** time of a credential application, do one of the following:

- **Task scheduled globally:** In the **Manage Credentials** window, hover your cursor over the horizontal ellipsis icon next to the credential name and choose **Apply**, and then click **Apply**.

- **Task scheduled from the main page for sites, buildings, or floors:** Return to the sites, buildings, or floors for which the task was originally scheduled and click **Apply** on the corresponding credential card.

Note You cannot change the time zone.

Configure IP Address Pools

Cisco DNA Center supports IPv4 and IPv6 dual-stack IP pools.

You can manually create IPv4 and IPv6 address pools.

You can also configure Cisco DNA Center to communicate with an external IP address manager. For more information, see the [Cisco DNA Center Administrator Guide](#).

Step 1 Click the menu icon () and choose **Design > Network Settings > IP Address Pools**.

Step 2 Click **Add** and complete the required fields in the **Add IP Pool** window.

If you have configured Cisco DNA Center to communicate with an external IP address manager, you cannot create an IP pool that overlaps an existing IP address pool in the external IP address manager.

Step 3 Click **Save**.

The newly added pool appears in the IP Address Pools table. You can click the **IPv4** or **IPv6** option in the **SUBNET TYPE** area if you prefer to view only the IPv4 or IPv6 address pools.

Note When you edit an IP address pool and make DHCP changes, you do not need to reprovision devices using that IP address pool.

Import IP Address Pools from an IP Address Manager

You can import IP address pools from Bluecat or Infoblox.



Note The IP address pools cannot have subpools and cannot have any assigned IP addresses from the IP address pool.

You must configure Cisco DNA Center to communicate with an external IP Address Manager (IPAM). For more information, see the [Cisco DNA Center Administrator Guide](#).

Step 1 Click the menu icon () and choose **Design > Network Settings > IP Address Pools**.

Step 2 From the **Actions** drop-down list, choose **Import from IPAM Server** and complete the required fields.

Step 3 Enter a CIDR and then click **Retrieve** to get the list of IP pools available to import.

Step 4 Click **Select All** or choose the IP address pools to import, then click **Import**.

Import IP Address Pools from a CSV File

You can import IP address pools from a CSV file.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.

Step 2 From the **Actions** drop-down list, choose **Import from CSV File**.

Step 3 Click **Download Template** to download the latest sample file.

Step 4 Add the IP address pools to the file and save the file.

Step 5 Upload the CSV file by doing one of the following actions:

- a) Drag and drop the file to the drag and drop area.
- b) Click where it says "**click to select**" and select the file.

Step 6 Click **Import**.

Reserve an IP Address Pool

Before you begin

Ensure that one or more IP address pools have been created.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.

Step 2 From the left hierarchy tree, choose a site.

Step 3 Click **Reserve** and complete the following fields to reserve all or part of an available global IP address pool for the specific site:

- **IP Address Pool Name:** Unique name for the reserved IP address pool.
- **Type:** Type of IP address pool. For LAN automation, choose **LAN**. Options are:
 - **LAN:** Assigns IP addresses to LAN interfaces for applicable underlays.
 - **Management:** Assigns IP addresses to management interfaces.
 - **Service:** Assigns IP addresses to service interfaces.
 - **WAN:** Assigns IP addresses to WAN interfaces.
 - **Generic:** Used for all other network types.
- **IP Address Space:** IPv4 and IPv6 address pool from which you want to reserve all or part of the IP addresses.
- **CIDR Prefix/Number of IP Addresses:** IP subnet and mask address used to reserve all or part of the global IP address pool or the number of IP addresses you want to reserve. If you choose \64 as the **CIDR Prefix** for an IPv6

IP pool, the **SLAAC** option is checked. (When **SLAAC** is selected, the devices automatically acquire IP addresses without the need for DHCP servers.)

- **Gateway:** Gateway IP address.
- **DHCP Servers:** DHCP server IP address(es).
- **DNS Servers:** DNS server address(es).

Step 4 Click **Reserve**.

If you reserve both IPv4 and IPv6 address pools, which means the fabric is provisioned with a dual-stack IP pool, you cannot switch back to a single-stack IP pool if the IPv6 pool is already attached to a VN.

However, if the IPv6 pool is not attached to a VN, you can downgrade it from a dual-stack IPv6 to a single-stack IPv4 pool. To downgrade to a single stack, in the IP Address Pools window, click **Edit** for the dual-stack IP pool. In the **Edit IP Pool** window, uncheck the **IPv6** check box and click **Save**.

Edit IP Address Pools

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.

Step 2 From the left hierarchy tree, choose the required site.

Step 3 To edit all the IP address pools in bulk, do the following:

- a) From the **Actions** drop-down list, choose **Edit All**.
- b) Click **Yes** in the **Warning** message.
- c) In the **Edit IP Pool** window make the desired changes and click **Save**.

Step 4 To edit only the desired IP address pools, do the following:

- a) Choose the desired IP address pools and from the **Actions** drop-down list, click **Edit Selected**.
You can also click **Edit** corresponding to the chosen IP address pools.
- b) In the **Edit IP Pool** window make the desired changes and click **Save**.

Delete IP Address Pools

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.

Step 2 From the left hierarchy tree, choose the required site.

Step 3 To delete all the IP address pools in bulk, do the following:

- a) From the **Actions** drop-down list, choose **Delete All**.
- b) Click **Yes** in the **Warning** message.

Step 4 To delete only the desired IP address pools, do the following:

- a) Choose the desired IP address pools and from the **Actions** drop-down list, click **Delete Selected**.

You can also click **Delete** corresponding to the chosen IP address pools.

- b) Click **Yes** in the **Warning** message.
-

Clone an IP Address Pool

You can clone an existing IP address pool at the site level. When you clone an IP address pool, the DHCP server and DNS server IP addresses are automatically filled.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.
 - Step 2** From the left hierarchy tree, choose the required site.
 - Step 3** Locate the desired IP address pool and, in the **Actions** area, click **Clone**.
 - Step 4** In the **Clone IP Pool** window, do the following:
 - a) Optionally, edit the pool name. (You cannot edit the Type, IP Address Space, or Global Pool values, which are inherited from the pool from which you are cloning.)
 - b) Edit the CIRD prefix values as necessary.
 - c) Click **Clone**.
-

Release IP Address Pools

You can release single-stack and dual-stack pools that are reserved at the site level.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.
 - Step 2** From the left hierarchy tree, choose the required site.
 - Step 3** To release all the IP address pools in bulk, do the following:
 - a) From the **Actions** drop-down list, choose **Release All**.
 - b) Click **Yes** in the **Warning** message.
 - c) At the prompt, click **Release**.
 - Step 4** To release only the desired IP address pools, do the following:
 - a) Choose the desired IP address pools and from the **Actions** drop-down list, click **Release Selected**.
 - b) At the prompt, click **Release**.
-

View IP Address Pools

This procedure shows how to view 10 or more IP address pools in table view and tree view.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > IP Address Pools**.
- Step 2** From the left hierarchy tree, choose the required site.

- Step 3** Use the toggle button to switch between the table view and tree view.
- When the view contains 10 or more IP address pools, by default the GUI displays the pools in the table view.
 - When the view contains fewer than 10 IP address pools, by default the GUI displays the pools in the tree view.
- Note** Toggling between the table and tree map view is based on the pool count not on the user selection on the UI.
- Tree view applies to the Global pool and site pool.
- Step 4** The **IP Address Pools** table view displays a list of IP address pools based on **Name**, **Type**, **IPv4 Subnet**, **IPv4 Used**, **IPv6 Subnet**, **IPv6 Used**, and **Actions**.
- Note**
- Hover your cursor over the **i** icon next to the **IPv4 Used** and **IPv6 Used**. A tooltip displays more information about **IPv4 Used**, **IPv6 Used**, **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP address pool.
 - In the **IPv4** and **IPv6** columns, hover your cursor over the **i** icon next to the corresponding used percentage of **IPv4** and **IPv6** for a given IP address pool. A tooltip displays the percentage of **Free**, **Unassignable**, **Assigned**, and **Default Assigned** IP addresses.
- Step 5** In the table view, click the **IPv4 only** or **Dual-Stack** option in the **Subnet Type** area if you prefer to view only the **IPv4** or **Dual-Stack** address pools.
- Step 6** In the tree view, hover your cursor over the IP address pool that you are interested in, and click to view the slide-in pane which contains the following information:
- Subnet type of an IP address pool.
 - Percentage of available IP addresses along with **Pool CIDR**, **Gateway**, **DHCP Server(s)**, and **DNS Server(s)** under the respective pool.
 - Percentage of used IP addresses under the respective pool.
- Step 7** In the **Used** area, click **Assigned** to view the list of assigned IP addresses to a device filtered based on **Device Name**, **IP Address**, and **Site**.
- Step 8** Click **Unassignable** to view the list of unassigned IP addresses which cannot be assigned to a device filtered based on **Device Name**, **IP Address**, and **Site**.
- Step 9** Click **Edit** to edit an IP address pool.
- Step 10** Click **Release** to release an IP address pool.
- Note**
- In the side bar for a global pool, you can view the usage of a given pool across all the child pool.
 - Global and site IP address pool can have blocklisted IP addresses.
 - Subpools cannot have blocklisted IP addresses.
 - Cisco DNA Center rejects the IP address pool creation request of a CIDR address pool if it contains blocklisted IP addresses.
 - In the next free IP address pools request, Cisco DNA Center skips the blocklisted IP addresses to find the next IP address free pool.

Step 11 (Optional) In the side bar click **Export** to export the table data.

Configure Service Provider Profiles

You can create a service provider (SP) profile that defines the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class service models. After you create an SP profile, you can assign it to an application policy and to the WAN interfaces in the application policy scope, including setting the subline rate on the interface, if needed.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings > SP Profiles**.

Step 2 In the **QoS** area, click **Add**.

Step 3 In the **Profile Name** field, enter a name for the SP profile.

Step 4 From the **WAN Provider** drop-down list, enter a new service provider, or choose an existing one.

Step 5 From the **Model** drop-down list, choose a class model: **4 class**, **5 class**, **6 class**, and **8 class**.

For a description of these classes, see [Service Provider Profiles, on page 593](#).

Configure Global Wireless Settings

Global wireless network settings include settings for Service Set Identifiers (SSIDs), wireless interfaces, RF, and sensors.



Note You can create a wireless sensor device profile for only Cisco Aironet 1800s Active Sensor devices.

Create SSIDs for an Enterprise Wireless Network

The following procedure describes how to configure SSIDs for an enterprise wireless network.



Note The SSIDs are created at the global level. Sites, buildings, and floors inherit settings from the global level.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **SSID** table, hover your cursor over **Add**, and choose **Enterprise**.

Step 5 In the **Wireless SSID** workflow, complete the **Basic Settings** setup:

- a) If the **Sensor** toggle button is available, ensure that it's disabled.
- b) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.
- c) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

Based on the WLAN profile name, Cisco DNA Center automatically generates the policy profile name for Cisco Catalyst 9800 Series Wireless Controller.

- d) In the **Wireless Option** settings, click one of the following radio buttons:
 - **Multi band operation (2.4 GHz, 5 GHz, 6GHz)**: The WLAN is created for 2.4 GHz, 5 GHz, and 6 GHz, and band select is disabled.
 - **Multi band operation with band select**: The WLAN is created for 2.4 GHz, 5 GHz, and 6 GHz, and band select is enabled.
 - **5GHz only**: The WLAN is created for 5 GHz, and band select is disabled.
 - **2.4GHz only**: The WLAN is created for 2.4 GHz, and band select is disabled.
 - **6GHz Only**: The WLAN is created for 6 GHz, and band select is disabled.
- e) From the **Primary Traffic Type** drop-down list, choose one of the following options:
 - **VoIP (Platinum)**: QoS on the wireless network is optimized for wireless voice and data traffic.
 - **Video (Gold)**: QoS on the wireless network is optimized for video traffic.
 - **Best Effort (Silver)**: QoS on the wireless network is optimized for wireless data traffic only.
 - **Non-real Time (Bronze)**: QoS on the wireless network is optimized for low-bandwidth usage.
- f) In the **SSID STATE** settings, click the toggle buttons to enable or disable the following settings:
 - **Admin Status**: Use this toggle button to turn on or turn off the radios on the APs. When the **Admin Status** is disabled, the APs remain associated with the wireless controller and are accessible, and the APs still require licenses.
 - **Broadcast SSID**: Use this toggle button to enable or disable the visibility of the SSID to all the wireless clients within range.

Step 6

Complete the **Security Settings** setup:

- a) For **Level of Security**, choose the encryption and authentication type for the network. The sites, buildings, and floors inherit settings from the Global hierarchy. You can override the level of security at the site, building, or floor level.
 - **Enterprise**: You can configure both **WPA2** and **WPA3** security authentication by checking the respective check boxes.

Note Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP).

WPA3 is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher-grade security protocols for sensitive data networks.

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.

- **Personal:** You can configure both **WPA2** and **WPA3** security authentication by checking the respective check boxes. By default, the **WPA2** check box is enabled. If you choose **Personal**, enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between the clients and authentication server.

Note WPA3-Personal brings better protection to individual users by providing more robust password-based authentication, making the brute-force dictionary attack much more difficult and time-consuming.

For WPA2-Personal, you can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floors inherit the new settings. For information, see [Preshared Key Override, on page 213](#).

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.

(Optional) For WPA2-Personal, do the following to configure multi-preshared key (MPSK) support:

1. Click **Configure MPSK**.
2. In the **Configure MPSK** dialog box, click **Add** to an MPSK. You can add up to five MPSKs.
3. From the **Priority** drop-down list, choose a priority.

Note If the priority 0 key is not configured in central web authentication (CWA) Flex mode, client connection to the WLAN may fail.

4. From the **Passphrase Type** drop-down list, choose a passphrase type.
5. In the **Passphrase** field, enter a passphrase.
6. Click **Save**.

MPSK is not supported on Cisco AireOS Wireless Controllers. MPSK applies to Layer 2 security configuration for WPA2- Personal.

- **Open Secured:** From the **Assign Open SSID** drop-down list, choose an open SSID to redirect the clients to an open-secured SSID. The open-secured policy provides the least security.

Note Fast Transition is not applicable for open-secured SSID.

Since open-secured SSID depends on open SSID, you must have enabled anchor on open SSID before enabling it on open-secured SSID.

- **Open:** The open policy provides no security. It allows any device to connect to the wireless network without any authentication.

b) For **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA** to add and configure the AAA servers for the enterprise wireless network SSID.

For more information, see [Configure AAA Server for an Enterprise Wireless Network, on page 215](#).

c) Check the **AAA Override** check box to enable the AAA override functionality.

By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.

d) Check one or more of the following check boxes:

- **Fast Lane:** Check this check box to enable fastlane capabilities on the network.

Note By enabling fastlane, you can set the iOS devices to receive an optimized level of wireless connectivity and enhanced QoS.

- **Identity PSK** (for Personal Layer 2 Security): Check this check box to enable unique preshared keys that can be created for individuals or groups of users in the SSID.

- **MAC Filtering:** Check this check box to enable MAC-based access control or security on the wireless network.

Note When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.

- **Deny RCM Clients:** Check this check box to deny clients with randomized MAC addresses.

- **Enable Posture:** Check this check box to enable posture assessment. The **Pre-Auth ACL List Name** drop-down list appears when you enable posture. Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients' access to protected areas of a network.

- **Pre-Auth ACL List Name:** From the drop-down list, choose the ACL list name that you already created to map with the SSID.

Note AAA configuration is mandatory for posturing. Click **Configure AAA** to add AAA servers for the enterprise wireless network SSID.

e) Click **Next**.

Step 7

Complete the **Advance Settings** setup:

a) For **Fast Transition (802.11r)**:

- Choose **Adaptive**, **Enable**, or **Disable** mode.

Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

- Check the **Over the DS** check box to enable fast transition over a distributed system. By default, fast transition over a distributed system is disabled.

b) For **MFP Client Protection**, choose **Optional**, **Required**, or **Disabled**.

Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between APs and clients. MFP provides both infrastructure and client support.

By default, **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and the client is also configured for WPA2 and supports CCXv5 MFP).

c) For **Protected Management Frame (802.11w)**, choose the required option.

Note The options available under **Protected Management Frame (802.11w)** vary based on the settings that you chose under **Level of Security**. The following options may be available:

- **Optional**
- **Required**
- **Disabled**

d) For **11K**:

- **Neighbor List**: Check this check box to configure all the 11k-capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

Note To facilitate roaming, a 11k-capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with the Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for the next roam from the response frame.

- **Session Timeout**: Check this check box to set the maximum time for a client session to remain active before reauthorization.

Note By default, **Session Timeout** is enabled with a timeout of 1800 seconds.

- **Client Exclusion**: Check this check box to set the client exclusion timer.

Note When a user fails to authenticate, the wireless controller excludes the client from connecting. The client is not allowed to connect to the network until the exclusion timer expires. By default, **Client Exclusion** is enabled with a timeout of 180 seconds.

e) For **11v BSS Transition Support**:

- **BSS Max Idle Service**: Check this check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from APs to the client.

Note The BSS Max idle period is the time frame during which an AP doesn't disassociate a client because of nonreceipt of frames from the connected client.

- **Client User Idle Timeout**: Check this check box to set the user idle timeout for a WLAN.

Note If the data sent by the client is more than the threshold quota specified as the user idle timeout, the client is considered to be active and the wireless controller begins another timeout period.

By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

- **Directed Multicast Service:** Check this check box to enable directed multicast service.

Note By default, **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer time and saves the battery power.

- f) For **Radius Client Profiling**, use this toggle button to enable or disable RADIUS profiling on a WLAN.

Note At least one AAA or PSN server is required to enable this feature.

- g) (Optional) For **NAS-ID**:

1. From the **NAS-ID Opt** drop-down list, choose the required type of network access server identifier (NAS ID).

To specify a custom script for the NAS ID, choose **Custom Option** from the **NAS-ID Opt** drop-down list and enter the custom script in the corresponding **Custom Script for Opt** field. You can enter up to 31 alphanumeric characters, special characters, and spaces for the custom script. Cisco DNA Center doesn't support the special characters ? " < and trailing spaces for the custom script.

Note Cisco DNA Center supports NAS ID with custom script only for Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.7 or later.

2. (Optional) Click + to add another NAS ID. You can add up to three NAS IDs.

Note Cisco DNA Center applies only one NAS ID for Cisco AireOS Wireless Controllers. You can overwrite the NAS ID at the site-level from the **Design > Network Settings > Wireless** window.

- h) **Configure CCKM:** Use this toggle button to enable CCKM as the authentication key management option in Cisco DNA Center.

- **Timestamp Tolerance:** This field is visible only if you enable CCKM. Enter the CCKM tolerance level. CCKM tolerance level is not applicable for the Cisco AireOS Wireless Controller platform.

Note You can configure CCKM only if SSID has Layer 2 security as Enterprise in WPA2 or WPA2+WPA3.

- i) (Optional) Under **Configure Client Rate Limit**, enter a value for the client rate limit in bits per second. The valid range is from 8000 through 10000000000. The value must be a multiple of 500.

Note This configuration is not applicable for Cisco AireOS Wireless Controllers. To configure client rate limit for Cisco AireOS Wireless Controllers, click the menu icon (≡) and choose **Tools > Model Config Editor > Wireless > Advanced SSID Configuration**. For more information, see [Create a Model Config Design for Advanced SSID, on page 315](#).

Following are the valid ranges for client rate limit on Cisco IOS XE devices:

- The valid range for Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, and Cisco Catalyst 9800-80 Wireless Controller is from 8000 through 67000000000 bits per second.
- The valid range for Cisco Catalyst 9800-CL Wireless Controller is from 8000 through 10000000000 bits per second.

- The valid range for Cisco Embedded Wireless Controller on Catalyst Access Points is from 8000 through 2000000000 bits per second.
- The valid range for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches is from 8000 through 100000000000 bits per second.

- j) (Optional) Use the **Coverage Hole Detection** toggle button to enable or disable the coverage hole detection functionality.
- k) Click **Next**.

Step 8 Complete the **Associate SSID to Profile** setup:

- a) From the left pane, select a profile and click **Associate Profile**.

If you don't have a profile, click **Add Profile** and configure the profile settings. For information, see [Create Network Profiles for Wireless, on page 281](#).

- b) Click **Next**.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Save**.

The SSID is created.

Preshared Key Override

SSIDs are created at the Global hierarchy. The sites, buildings, and floors inherit settings from the Global hierarchy. You can override a preshared key (PSK) at the site, building, or floor level. If you override a PSK at the building level, the subsequent floor inherits the new setting.


Step 1 Click the menu icon (☰) and choose **Design > Network Settings > Wireless**.

Step 2 From the left hierarchy tree, choose the site, building, or floor to edit the PSK.

Step 3 Under **Enterprise Wireless**, click the **Passphrase** field, and enter a new passphrase for the PSK SSID.

Step 4 Click **Save**.

A success message saying `Passphrase for the SSID(s) updated successfully` is displayed.




Hover your cursor over the inherit icon  next to the SSID to view the origin of this setting.

Step 5 To reset the PSK override, check the check box of the PSK SSID on the site, building, or floor and click **Delete**. The PSK is reset to the global passphrase value.

Create Pre-Auth Access Control Lists

Using the Pre-Authentication ACL feature, you can create a pre-authentication ACL for web authentication to allow certain types of traffic before authentication is complete. This ACL is referenced in the access-accept of Cisco Identity Services Engine (ISE) and defines the traffic that is permitted and the traffic that is denied by the ACL. After ACLs are configured on the Cisco Wireless Controller, they can be applied to the management interface, the AP-manager interface, any of the dynamic interfaces, or a WLAN to control data

traffic to and from wireless clients or to the controller central processing unit (CPU) to control all traffic destined for the CPU. You can configure both IPv4 and IPv6 ACLs.

- Step 1** Click the menu icon () and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** Under the **Pre-Auth Access Control Lists** area, click **Add** to create a new pre-auth ACL.
- Step 5** In the **New Pre-Auth ACL** slide-in pane, configure the following:
- In the **Pre-Auth ACL List Name** field, enter a name for the ACL list.
 - In the **Pre-Auth ACL Name** field, enter a name for the pre-auth ACL.
 - Click the **IP Addresses** tab and choose the ACL type you are creating: **IPv4** or **IPv6**.
- Step 6** Click the **IP Addresses** tab and choose the ACL type you are creating: **IPv4** or **IPv6**.
- From the **Protocol** drop-down list, choose the protocol ID of the IP packets to be used for this ACL. These are the protocol options: **Any**, **TCP**, or **UDP**.
 - In the **Source Port** field, enter the source port number. The range is from 0 through 65535. The port options are used by applications that send and receive data to and from the networking stack. Some ports are designated for certain applications such as Telnet, SSH, HTTP, and so on.
 - In the **Source IP Address** field, enter the IP address and netmask of the source. If you are configuring an IPv6 ACL, enter the IPv6 address and prefix length of the source in the Source IP Address field.
 - From the **Source Subnet** drop-down list, choose a value for the source subnet.
 - In the **Destination Port**, enter the destination port number.
 - In the **Destination IP Address**, enter the IP address and netmask of the destination. If you are configuring IPv6 ACL, enter the IPv6 address and prefix length of the destination.
 - From the **Destination Subnet** drop-down list, choose a value for the destination subnet.
 - To add multiple rules, click the  icon. You can add up to 256 rules.
- Step 7** Click the **Walled Garden URLs** tab to add specific URLs to the allowed list for web authentication of captive portal and walled garden. Authentication is not required to access the allowed list of URLs. When you try to access sites that are not in the allowed list, you are redirected to the Login page.
- Step 8** In the **URL** field, enter the URL and click  to add the URL to the allowed list for web authentication. You can add up to 32 URL entries.
- Step 9** Click **Save**.
- Step 10** Map the ACL with the SSID while creating SSIDs for an enterprise wireless network.
-

Configure AAA Server for an Enterprise Wireless Network

Before you begin

- Make sure you have defined the AAA server under **System Settings > External Services > Authentication and Policy Servers**.
- You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions, and the appropriate RBAC scope to perform this procedure.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 From the **SSID** table, in the **Action** column, click **Configure AAA** against an SSID for which you want to configure the AAA server.

Step 5 From the **Configure Authentication and Authorization Server** drop-down list of the **Configure AAA Server** slide-in pane, you can either search for a server IP address by entering its name in the **Search** field or choose the AAA IP address.

- Note**
- The **Configure AAA** option is not supported for the Mobility Express (ME) devices.
 - Effective with Release 2.3.5.3, you must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Cisco DNA Center pushes the **aaa authentication dot1x default local** command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.

Step 6 Click + to add an **Additional Server**.

- Note** You can configure a maximum of six AAA servers for an SSID of enterprise wireless network.

Step 7 From the **Additional Server** drop-down list, choose the server IP address.

Step 8 To use the AAA server for accounting, check the **Copy Same Servers for Accounting** check box.

- Note** Effective with Release 2.3.5.3, you must configure an accounting server for an SSID to push the accounting configuration for the SSID.

Step 9 To configure a different accounting server for an SSID, do the following:

- a) From the **Configure Accounting Server** drop-down list, you can either search for a server IP address by entering its name in the **Search** field or choose the accounting server IP address.
- b) Click + to add an **Additional Server**.

- Note** You can configure a maximum of six accounting servers for an SSID of enterprise wireless network.

c) From the **Additional Server** drop-down list, choose the server IP address.

Step 10 Click **Configure**.

Note Cisco DNA Center allows you to override the set of AAA server configurations for the SSID at the site level. For each set of overridden AAA settings per SSID, Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Cisco DNA Center creates the new WLAN profiles equal to the number of floors.

You must reprovision the device to override the AAA servers at the site level. See [Wireless Device Provisioning Overview, on page 389](#).

Create SSIDs for a Guest Wireless Network

This procedure explains how to create SSIDs for a guest wireless network.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **SSID** table, hover your cursor over **Add**, and choose **Guest**.

Step 5 In the **Wireless SSID** workflow, complete the **Basic Settings** setup:

- a) In the **Wireless Network Name (SSID)** field, enter a unique name for the wireless network.
- b) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

Based on the WLAN profile name, Cisco DNA Center automatically generates the policy profile name for Cisco Catalyst 9800 Series Wireless Controller.

- c) In the **Wireless Option** setting, click one of the following radio buttons:
 - **Multi band operation (2.4 GHz, 5 GHz, 6GHz)**: The WLAN is created for 2.4 GHz, 5 GHz, and 6 GHz, and band select is disabled.
 - **Multi band operation with band select**: The WLAN is created for 2.4 GHz, 5 GHz, and 6 GHz, and band select is enabled.
 - **5GHz only**: The WLAN is created for 5 GHz, and band select is disabled.
 - **2.4GHz only**: The WLAN is created for 2.4 GHz, and band select is disabled.
 - **6GHz Only**: The WLAN is created for 6 GHz, and band select is disabled.
- d) From the **Primary Traffic Type** drop-down list, choose one of the following options:
 - **VoIP (Platinum)**: QoS on the wireless network is optimized for wireless voice and data traffic.
 - **Video (Gold)**: QoS on the wireless network is optimized for video traffic.
 - **Best Effort (Silver)**: QoS on the wireless network is optimized for wireless data traffic only.
 - **Non-real Time (Bronze)**: QoS on the wireless network is optimized for low-bandwidth usage.
- e) In the **SSID STATE** settings, click the toggle buttons to enable or disable the following settings:

- **Admin Status:** Use this toggle button to turn on or turn off the radios on the APs. When the **Admin Status** is disabled, the APs remain associated with the wireless controller and are accessible, and the APs still require licenses.
- **Broadcast SSID:** Use this toggle button to enable or disable the visibility of the SSID to all the wireless clients within range.

Step 6

Complete the **Security Settings** setup:

a) For the **L2 Security** setting, choose the L2 encryption and authentication type:

- **Enterprise:** You can configure either the **WPA2** or the **WPA3** security authentication type by checking the respective check boxes. By default, the **WPA2** check box is enabled.

Note Wi-Fi Protected Access (WPA2) uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Fast transition is applicable for enterprise WPA2 SSID.

WPA3 security authentication is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher grade security protocols for sensitive data networks.

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.

- **Personal:** You can configure both **WPA2** and **WPA3** or configure **WPA2** and **WPA3** individually by checking the respective check boxes.

Note WPA3-Personal security authentication brings better protection to individual users by providing more robust password-based authentication. This makes the brute-force dictionary attack much more difficult and time-consuming.

Enter the passphrase key in the **Pass Phrase** field. This key is used as the pairwise master key (PMK) between the clients and the authentication server.

For multiband operation using only 2.4-GHz and 5-GHz bands, you must enable WPA2 (WPA3 is optional). For multiband operation using 2.4-GHz, 5-GHz, and 6-GHz bands, you must enable WPA3 and disable WPA2 for the 6-GHz band to be operational on the devices running Cisco IOS Release 17.7 and later.

(Optional) For WPA2-Personal, do the following to configure multi-pre-shared key (MPSK) support:

1. Click **Configure MPSK**.
2. In the **Configure MPSK** dialog box, click **Add** to an MPSK. You can add up to five MPSKs.
3. From the **Priority** drop-down list, choose a priority.

Note If the priority 0 key is not configured in central web authentication (CWA) Flex mode, client connection to the WLAN may fail.

4. From the **Passphrase Type** drop-down list, choose a passphrase type.
5. In the **Passphrase** field, enter a passphrase.
6. Click **Save**.

MPSK is not supported on Cisco AireOS Wireless Controllers. MPSK applies to Layer 2 security configuration for WPA2- Personal.

- **Open Secured:** From the **Assign Open SSID** drop-down list, choose an open SSID to associate with the open SSID. Associating secures the open SSID. You must have an open SSID created before associating it with the open secured SSID.

Note Fast Transition is not applicable for open-secured SSID.

Since open-secured SSID depends on open SSID, you must have enabled anchor on open SSID before enabling it on open-secured SSID.

- **Open:** The open policy provides no security. It allows any device to connect to the wireless network without any authentication.

b) For the **L3 Security** setting, choose the L3 encryption and authentication type:

- **Web Policy:** Provides a higher level of L3 security.

For **Authentication Server**, configure these authentication server settings:

Authentication Server Type	Description
Central Web Authentication	<p>Use AAA server for central web authentication (CWA).</p> <p>(Optional) If you choose Cisco ISE for CWA, from the What kind of portal are you creating today? drop-down list, choose the type of portal you want to create:</p> <ul style="list-style-type: none"> • Self Registered: The guests are redirected to the self-registered guest portal to register by providing information to automatically create an account. • HotSpot: The guests can access the network without providing any credentials. <p>(Optional) If you choose Cisco ISE for CWA, from the Where will your guests redirect after successful authentication? drop-down list, choose where you want to redirect the guests after successful authentication:</p> <ul style="list-style-type: none"> • Success Page: The guests are redirected to an Authentication Success window. • Original URL: The guests are redirected to the URL that they had originally requested. • Custom URL: The guests are redirected to the custom URL that is specified here. Enter a redirect URL in the Redirect URL field.

Authentication Server Type	Description
<ul style="list-style-type: none"> • Web Authentication Internal • Web Authentication External 	<p>Web authentication or Web Auth is a Layer 3 security method that allows a client to pass Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) traffic only until they have passed some form of authentication.</p> <p>For web authentication internal, the client is redirected to a page that is constructed by the Cisco Wireless Controller.</p> <p>For web authentication external, the client is redirected to the specified URL. Enter a redirect URL in the Web Auth Url field.</p>
<ul style="list-style-type: none"> • Web Passthrough Internal • Web Passthrough External 	<p>Web passthrough is a solution that is used for guest access and requires no authentication credentials. In web passthrough authentication, wireless users are redirected to the usage-policy page when they use the internet for the first time. After accepting the policy, users are allowed to use the internet.</p>

- **Open:** There is no security at the Layer 3 level and any device can connect to the SSID.

c) If you choose **Web Authentication Internal**, **Web Authentication External**, **Web Passthrough Internal**, or **Web Passthrough External**, for **Timeout Settings for sleeping clients** settings, choose the authentication for sleeping clients:

- **Always authenticate:** Enables authentication for sleeping clients.
- **Authenticate after:** Enter the duration for which sleeping clients are to be remembered before reauthentication becomes necessary. The valid range is from 10 minutes through 43200 minutes, and the default duration is 720 minutes.

Note Clients with guest access and web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before reauthentication becomes necessary. The valid range is from 10 minutes through 43200 minutes; the default is 720 minutes. You can configure the duration on a WLAN and on a user group policy that is mapped to the WLAN. The sleeping timer becomes effective after the idle timeout. If the client timeout is less than the time configured on the sleeping timer of the WLAN, the lifetime of the client is used as the sleeping time.

d) For **Authentication, Authorization, and Accounting Configuration**, click **Configure AAA** to add and configure the AAA servers for the guest wireless network SSID.

For more information, see [Configure AAA Server for a Guest Wireless Network, on page 223](#).

e) Check the **AAA Override** check box to enable the AAA override functionality.

By default, this check box is dimmed. You must configure an AAA server using the **Configure AAA** option to use this check box.

f) Check one or more of the following check boxes:

- **Fast Lane:** Check this check box to enable fastlane capabilities on the network.

Note By enabling fastlane, you can configure the iOS devices to receive an optimized level of wireless connectivity and enhanced QoS.

- **Identity PSK** (for Personal L2 Security): Check this check box to enable unique preshared keys that can be created for individuals or groups of users in the SSID.
- **MAC Filtering**: Check this check box to enable MAC-based access control or security in the wireless network.
 - Note** When MAC filtering is enabled, only the MAC addresses that you add to the wireless LAN are allowed to join the network.
- **Deny RCM Clients**: Check this check box to deny clients with randomized MAC addresses.

g) Click **Next**.

Step 7

Complete the **Advance Settings** setup:

a) For **Fast Transition (802.11r)**:

- Choose **Adaptive**, **Enable**, or **Disable** mode.

Note 802.11r allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

- Check the **Over the DS** check box to enable fast transition over a distributed system. By default, fast transition over a distributed system is disabled.

b) For **MFP Client Protection**, choose **Optional**, **Required**, or **Disabled**.

Note Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between APs and clients. MFP provides both infrastructure and client support.

By default, **Optional** is selected. If you choose **Required**, the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller, and the client is also configured for WPA2 and supports CCXv5 MFP).

c) For **Protected Management Frame (802.11w)**, choose the required option.

Note The options available under **Protected Management Frame (802.11w)** vary based on the settings that you chose under **Level of Security**. The following options may be available:

- **Optional**
- **Required**
- **Disabled**

d) For **11K**:

- **Neighbor List**: Check this check box for all the 11k-capable clients to request a neighbor report about the known neighboring APs that are candidates for roaming.

Note To facilitate roaming, a 11k-capable client that is associated with an AP sends a request to a list of neighboring APs. The request is sent in the form of an 802.11 management frame, which is known as an action frame. The AP responds with a list of neighbor APs on the same WLAN with the Wi-Fi channel numbers. The response is also an action frame. The client identifies the AP candidates for the next roam from the response frame.

- **Session Timeout:** Check this check box to set the maximum time for a client session to remain active before reauthorization.

Note By default, **Session Timeout** is enabled with a timeout of 1800 seconds.

- **Client Exclusion:** Check this check box to set the client exclusion timer.

Note When a user fails to authenticate, the wireless controller excludes the client from connecting. The client is not allowed to connect to the network until the exclusion timer expires. By default, **Client Exclusion** is enabled with a timeout of 180 seconds.

e) For **11v BSS Transition Support:**

- **BSS Max Idle Service:** Check this check box to set the idle period timer value. The idle period timer value is transmitted using the association and reassociation response frame from the APs to the client.

Note The BSS Max idle period is the timeframe during which an AP doesn't disassociate a client because of nonreceipt of frames from the connected client.

- **Client User Idle Timeout:** Check this check box to set the user idle timeout period for a WLAN.

Note If the data sent by the client is more than the threshold quota specified as the user idle timeout period, the client is considered to be active and the wireless controller refreshes for another timeout period.

By default, **Client User Idle Timeout** is enabled with a user idle timeout of 300 seconds.

- **Directed Multicast Service:** Check this check box to enable directed multicast service.

Note By default, **Directed Multicast Service** is enabled. Using the Directed Multicast Service (DMS), the client requests APs to transmit the required multicast packets as unicast frames. This allows clients to sleep for a longer time and saves the battery power.

f) (Optional) For **NAS-ID:**

1. From the **NAS-ID Opt** drop-down list, choose the required type of network access server identifier (NAS ID).

(Optional) To specify a custom script for the NAS ID, choose **Custom Option** from the **NAS-ID Opt** drop-down list and enter the custom script in the corresponding **Custom Script for Opt** field. You can enter up to 31 alphanumeric characters, special characters, and spaces for the custom script. Cisco DNA Center doesn't support the special characters ? " < and trailing spaces for the custom script.

Note Cisco DNA Center supports NAS ID with custom script only for Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.7 or later.

2. (Optional) Click + to add another network access server identifier. You can add up to three NAS IDs.

Note Cisco DNA Center applies only one NAS ID for Cisco AireOS Controllers. You can overwrite the NAS ID at the site-level from the **Design > Network Settings > Wireless** window.

- g) (Optional) Under **Configure Client Rate Limit**, enter a value for the client rate limit in bits per second. The valid range is from 8000 through 100000000000. The value must be a multiple of 500.

Note This configuration is not applicable for Cisco AireOS Wireless Controllers. To configure client rate limit for Cisco AireOS Wireless Controllers, click the menu icon (≡) and choose **Tools > Model Config Editor > Wireless > Advanced SSID Configuration**. For more information, see [Create a Model Config Design for Advanced SSID, on page 315](#).

Following are the valid ranges for client rate limit on Cisco IOS XE devices:

- The valid range for Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, and Cisco Catalyst 9800-80 Wireless Controller is from 8000 through 67000000000 bits per second.
 - The valid range for Cisco Catalyst 9800-CL Wireless Controller is from 8000 through 10000000000 bits per second.
 - The valid range for Cisco Embedded Wireless Controller on Catalyst Access Points is from 8000 through 20000000000 bits per second.
 - The valid range for Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches is from 8000 through 100000000000 bits per second.
- h) (Optional) Use the **Coverage Hole Detection** toggle button to enable or disable the coverage hole detection functionality.
- i) Click **Next**.

Step 8

Complete the **Associate SSID to Profile** setup:

- a) Click a profile from the left pane.
- b) If you don't have a profile, click **Add Profile** and then configure the profile settings:

- **Profile Name:** Enter a name for the wireless profile.
- (Optional) **WLAN Profile Name:** Enter a name for the WLAN profile.


Based on the WLAN profile name, Cisco DNA Center automatically generates the policy profile name for Cisco Catalyst 9800 Series Wireless Controller.

Note When an SSID is associated with a network profile, Cisco DNA Center uses this WLAN profile name during provisioning. If you need to associate an SSID with multiple network profiles, we recommend that you enter a unique WLAN profile name for the SSID across all network profiles to prevent provisioning failure.


- **Fabric:** Specify whether the SSID is fabric or nonfabric.

Note A fabric SSID is a wireless network, which is a part of Software Defined-Access (SD-Access). SD-Access is a solution that automates and simplifies configuration, policy, and troubleshooting of wired and wireless networks. With fabric SSID, it's mandatory to have SD-Access. Nonfabric is a traditional wireless network that doesn't require SD-Access.

For a nonfabric SSID, choose the following:

- **Interface:** From the **Interface Management** drop-down list, choose an interface or click the plus icon  to add a new wireless interface.

Note This is the VLAN ID that is associated with the wireless interface.

- **VLAN Group:** From the **VLAN Group Name** drop-down list, choose a VLAN group or click the plus icon  to add a VLAN group.

- **Do you need Anchor for this SSID?:** Choose whether the SSID is an anchor or not.

If you choose **Yes**, from the **Select Anchor Group** drop-down list, choose an anchor group for the SSID. For more information about anchor groups, see [Create an Anchor Group, on page 252](#).

- **Flex Connect Local Switching:** Check this check box to enable local switching for the WLAN. When you enable local switching, any FlexConnect AP that advertises this WLAN is able to locally switch data packets.

Note If you have enabled **Flex Connect Local Switching** for an SSID, then all the APs on that particular floor where the network profile is mapped switch to FlexConnect mode.

c) Click **Associate Profile** to choose the profile.

d) Click **Next**.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)


Step 10 To save the SSID settings, click **Save**.

The SSID is created.

Configure AAA Server for a Guest Wireless Network

Before you begin

- Make sure you have defined the AAA server under the **System Settings > External Services > Authentication and Policy Servers** window.
- You must have either administrator (ROLE_ADMIN) or policy administrator (ROLE_POLICY_ADMIN) permissions and the appropriate RBAC scope to perform this procedure.

Step 1 Click the menu icon () and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 From the **SSID** table, in the **Action** column, click **Configure AAA** of SSID for which you want to configure the AAA server.

Step 5 From the **Server** drop-down list of the **Configure AAA Server** slide-in pane, you can either search for a AAA IP address by entering its name in the **Search** field or choose AAA IP address.

- Note**
- You must configure at least one AAA or Policy Service Node (PSN) server for Central Web Authentication (CWA) SSIDs of guest wireless network.
 - Effective with Release 2.3.5.4, Cisco DNA Center-generated preauthentication ACLs are created only for the configured AAA or PSN servers for CWA SSIDs of guest wireless networks. If you upgrade to Release 2.3.5.4 from Release 2.3.5.3 or earlier, to ensure that there is no compliance mismatch, you must reprovision the wireless controller.
 - Cisco DNA Center allows you to map AAA server in any combination of identity services engine PSNs and third-party AAA IPs.
 - In the **Server** drop-down list, the **AAA** IP addresses and the PSN IP addresses are grouped in the corresponding sections.
 - The **Configure AAA** option is not supported for Mobility Express (ME) devices.
 - Effective with Release 2.3.5.3, you must configure an AAA server for an SSID to push the authentication configuration for the SSID. If an AAA server is not configured for the SSID, Cisco DNA Center pushes the **aaa authentication dot1x default local** command to the wireless controller and the default method list that points to local authentication is mapped to the SSID.

Step 6 Click + to add an **Additional Server**.

Note You can configure a maximum of six AAA servers for an SSID of guest wireless network.

Step 7 From the **Additional Server** drop-down list, choose the server IP address.

Step 8 (Optional) To delete a server or an additional server, click the delete icon next to each server.

Step 9 To use the AAA server for accounting, check the **Copy Same Servers for Accounting** check box.

Note Effective with Release 2.3.5.3, you must configure an accounting server for an SSID to push the accounting configuration for the SSID.

Step 10 To configure a different accounting server for an SSID, do the following:

- From the **Configure Accounting Server** drop-down list, you can either search for a server IP address by entering its name in the **Search** field or choose the accounting server IP address.
- Click + to add an **Additional Server**.

Note You can configure a maximum of six accounting servers for an SSID of guest wireless network.

- From the **Additional Server** drop-down list, choose the server IP address.

Step 11 Click **Configure**.

Note Cisco DNA Center allows you to override the set of AAA server configurations for the SSID at the site level. For each set of overridden AAA settings per SSID, Cisco DNA Center creates a new WLAN profile with the corresponding AAA servers mapped to it. If an SSID is overridden for different floors, and you make changes in the AAA servers, Cisco DNA Center creates the new WLAN profiles equal to the number of floors.

You must reprovision the device to override the AAA servers at the site level. See [Wireless Device Provisioning Overview, on page 389](#).

Create SSID Scheduler

You can create SSID scheduler to enable or disable WLAN based on time zone.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** In the **SSID** table, click **SSID Scheduler**.
- Step 4** In the **SSID Scheduler** window, click **Add**.
- Step 5** In the **Create Scheduler** slide-in pane, do the following:
- Enter a unique name for the SSID scheduler that you want to create.
 - Click **Client Deny** radio button for denying clients from joining SSID.
 - Click **Enable SSID** to schedule SSID broadcasting.
 - Choose the **Scheduler Type Daily, Weekly, or Monthly** and complete the required settings.
 - From the **Time Zone** drop-down list, choose the time zone.
 - Click **Save**.

The created SSID scheduler appears in the **SSID Scheduler** table.

- Step 6** To edit the SSID scheduler, do the following:
- From the **SSID Scheduler** table, choose the SSID scheduler and click **Edit**.
 - In the **Edit SSID Scheduler** slide-in pane, make the required changes and click **Save**.
- Step 7** To delete the SSID scheduler, choose the SSID scheduler and click **Delete**.
- Step 8** To view the details of SSID scheduler, choose the SSID scheduler and click **Scheduler History**.

Note To view the **Scheduler History**, you must install Assurance package.

What to do next

Enable the SSID scheduler for wireless controller. For more details, see [Add SSIDs to a Network Profile, on page 282](#).

Create a Wireless Interface

You can create wireless interfaces only in nonfabric deployments.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** From the **Wireless Interfaces** table, click **+Add**.
- Step 5** Configure the wireless interface settings in the **Create a Wireless Interface** slide-in pane:
- In the **Interface Name** field, enter the dynamic interface name.
 - In the **VLAN ID** field, enter the VLAN ID for the interface.

Step 6 Click **Save**.

The wireless interface is created and displayed in the **Wireless Interfaces** table.

Design and Provision Interface/VLAN Groups to Nonfabric Deployments

Cisco DNA Center allows you to configure networks with multiple broadcast domains through different VLANs. When the same set of APs broadcast the same WLAN, the broadcast domains are controlled through multiple VLANs on the same WLAN through interface groups.

Cisco DNA Center interface groups are logical groups of interfaces that 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 can be part of multiple interface groups. A WLAN can be associated with an interface or interface group.



Note The interface group name and the interface name cannot be the same.

The Cisco DNA Center VLAN group feature maps a WLAN to a single VLAN or multiple VLANs using VLAN groups. VLAN groups can be associated to policy profiles.

The following procedure explains how to design and provision the interface or VLAN groups for nonfabric deployments.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 For the **VLAN Group** table, click **Add**.

The **Add VLAN Group** slide-in pane is displayed.

Step 4 Enter a valid **VLAN Group Name**, select single or multiple interfaces from the list, and click **Save**.

Note If you select more than 15 interfaces, the selected interfaces might not be displayed correctly onscreen.

Step 5 In the **Edit Network Profile** page, the VLAN group is associated with the SSID.

For information on how to create an SSID, see [Create SSIDs for an Enterprise Wireless Network](#).

Step 6 To add more SSIDs to the VLAN group, click **Add SSID**.

Step 7 Choose **Interface** or **VLAN** group.

Step 8 Click the add icon to create a new interface or VLAN group.

Note Interface or VLAN group is not applicable for FlexConnect local switching.

Step 9 Click **Save**.

Step 10 In **Configure Interface and VLAN**, you can view the list of interface names, interface groups names, and other parameters required to configure the interface and VLAN.

Note An interface group cannot contain more than 64 interfaces.

- Step 11** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 12** Select the device.
- Step 13** From the **Actions** drop-down menu, choose **Provision > Provision Device**.
- Step 14** Review the details in the **Assign Site, Configuration, Model Configuration, Advanced Configuration, and Summary** screens. From each screen, click **Next** to advance to the next screen.
- Step 15** Click **Deploy**.
The **Provision Device** dialog box is displayed.
- Step 16** Choose **Now** and click **Apply**.
The message **Task Scheduled view status in Tasks** is displayed.
-

Create a Wireless Radio Frequency Profile

You can either use the default radio frequency profiles (LOW, TYPICAL, HIGH), or create custom radio frequency profiles.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** In the **Wireless Radio Frequency Profile** area, hover your cursor over **Add**, and choose **Basic RF Profile**.
- Step 5** In the **Profile Name** field of the **Create Wireless Radio Frequency Profile** window, enter the RF profile name.
- Step 6** Configure the following in the **2.4 GHz** tab:
- Ensure that the **2.4 GHz** toggle button is enabled.
- Note**
- For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **2.4 GHz** toggle button, Cisco DNA Center disables the Admin status of the **2.4 GHz** RF profile.
 - In Release 2.3.5.3, for Cisco AireOS Wireless Controller, if you disable the **2.4 GHz** toggle button, Cisco DNA Center disables the Admin status of the respective radios on all APs that use this RF profile. We recommend that you disable the Admin status using the **Configure Access Points** workflow. For more information, see [Configure AP Workflow, on page 716](#).
 - Effective with Release 2.3.5.4, for Cisco AireOS Wireless Controller, if you disable the **2.4 GHz** toggle button and reprovision the wireless controller or AP, Cisco DNA Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as **None**) and disables the Admin status of the corresponding radios on the APs.
 - For Cisco AireOS Wireless Controller, when you disable the Admin status for the 2.4-GHz band on the RF profile, Cisco DNA Center changes the XOR radio on the APs using that RF profile to manual 5-GHz mode. If you enable the Admin status later and reprovision the AP, Cisco DNA Center changes the radio to automatic mode enabling the usage of 2.4-GHz and 5-GHz bands, and monitor mode. So, if you want to disable the Admin status for the 2.4-GHz band on XOR-capable APs, we recommend that you disable the Admin status of the XOR radio using the **Configure Access Points** workflow. The Admin status configured using the **Configure Access Points** workflow isn't overwritten when the wireless controller or APs are reprovisioned. For more information, see [Configure AP Workflow, on page 716](#).

- b) Under **Parent Profile**, select **High**, **Medium (Typical)**, **Low**, or **Custom**. (The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates the profile configurations available in the device for 2.4-GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration**, the **Parent Profile** automatically changes to **Custom**.) Note that a new RF profile is created only for the selected custom profiles.

Note **Low**, **Medium (Typical)**, and **High** are the default RF profiles. If you select a default RF profile, the respective RF profile on the device is used, and the new RF profile is not created on wireless controller.

- c) **DCA Channel** dynamically manages channel assignment for an RF group and evaluates the assignments on a per-AP radio basis.
- Check the **Select All** check box to select DCA channels **1**, **6**, and **11**. Alternatively, check the individual check boxes next to the channel numbers.
 - Click **Show Advanced** to select the channel numbers under the **Advanced Options**.
 - Check the **Select All** check box to select DCA channels that are under **Advanced Options**, or check the check box next to the individual channel numbers. The available channel numbers are **2**, **3**, **4**, **5**, **7**, **8**, **9**, **10**, **12**, **13**, and **14**.

Note For Cisco AireOS Wireless Controller, Cisco DNA Center automatically configures the selected DCA channels in the global RRM DCA channel list.

Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- d) Under **Supported Data Rate**, configure the following:
- Check the **Enable 802.11b data rates** check box to enable the 802.11b data rates.
 - Use the slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48**, and **54**.
- e) Under **Mandatory Data Rates**, check the check boxes next to the individual data rates. You can choose up to two data rates. The available data rates are **6**, **9**, **12**, **18**, **24**, **36**, **48**, and **54**.
- The available data rates change depending on the data rates set under **Supported Data Rate**.
- f) Under **Tx Power Configuration**, set the power level and power threshold for an AP.

- **Power Level**: To determine whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm to 30 dBm and the default is -10 dBm.
- **TPC Power Threshold**: Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
- **RX SOP**: Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High**, **Medium**, **Low**, or **Auto** threshold values for each 802.11 band.

g) Under **Coverage Hole Detection**, configure the following:

Note You must enable global coverage hole detection in **Tools > Model Config Editor > Wireless > RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see [Create a Model Config Design for RRM General Parameters, on page 329](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

h) In the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note Maximum client limit is not supported on the Cisco AireOS Wireless Controller.

- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

i) Under **802.11ax**, configure the following spatial reuse parameters:

Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 7

Configure the following in the **5 GHz** tab:

a) Ensure that the **5 GHz** toggle button is enabled.

- Note**
- For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **5 GHz** toggle button, Cisco DNA Center disables the Admin status of the **5 GHz** RF profile.
 - In Release 2.3.5.3, for Cisco AireOS Wireless Controller, if you disable the **5 GHz** toggle button, Cisco DNA Center disables the Admin status of the respective radios on all APs that use this RF profile. We recommend that you disable the Admin status using the **Configure Access Points** workflow. For more information, see [Configure AP Workflow, on page 716](#).

Effective with Release 2.3.5.4, for Cisco AireOS Wireless Controller, if you disable the **5 GHz** toggle button and reprovision the wireless controller or AP, Cisco DNA Center creates the RF profile for the corresponding band and maps it to the AP group (instead of configuring it as **None**) and disables the Admin status of the corresponding radios on the APs.

- For Cisco AireOS Wireless Controller, when you disable the Admin status for the 5-GHz band on the RF profile, Cisco DNA Center changes the XOR radio on the APs using that RF profile to manual 2.4-GHz mode. If you enable the Admin status later and reprovision the AP, Cisco DNA Center changes the radio to automatic mode enabling the usage of 2.4-GHz and 5-GHz bands, and monitor mode. So, if you want to disable the Admin status for the 5-GHz band on XOR-capable APs, we recommend that you disable the Admin status of the XOR radio using the **Configure Access Points** workflow. The Admin status configured using the **Configure Access Points** workflow isn't overwritten when the wireless controller or APs are reprovisioned. For more information, see [Configure AP Workflow, on page 716](#).
- b) From the **Parent Profile** drop-down list, choose **High, Medium (Typical), Low, or Custom**. (The **Data Rate** and **Tx Configuration** fields change depending on the parent profile selected. For example, if you select **High**, it populates the configurations available in the device for 2.4 GHz. If you change any settings in the populated **Data Rate** and **Tx Configuration** fields, the **Parent Profile** automatically changes to **Custom**.) A new RF profile is created only for select custom profiles.

Note **Low, Medium (Typical), and High** are the default RF profiles. If you select a default RF profile, the respective RF profile that is already present in the device is used and the new RF profile is not created on wireless controller.

- c) From the **Channel Width** drop-down list, choose one of the channel bandwidth options: **Best, 20 MHz, 40 MHz, 80 MHz, or 160 MHz**.
- d) Check the **Zero Wait DFS** check box to allow APs with 5-GHz radio band to switch to a new channel without any waiting time.

Note Cisco DNA Center supports Zero wait DFS for Cisco Wireless Controllers running Cisco IOS XE Release 17.9.1 and later.

- e) Under **DCA Channel**, configure the following to manage channel assignments:

Note For Cisco AireOS Wireless Controller, Cisco DNA Center automatically configures the selected DCA channels in the global RRM DCA channel list.

Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- Check the **Select All** check box to select DCA channels **UNII-1 36-48, UNII-2 52-144, and UNII-3 149-173**. Alternatively, check the individual check boxes next to the channel numbers.

- Click **Show Advanced** to select the channel numbers for each band.
 - **UNII-1 36-48**: The channels available for UNII-1 band are **36, 40, 44, and 48**. Check the **UNII-1 36-48** check box to include all channels, or check an individual check box.
 - **UNII-2 52-144**: The channels available for UNII-2 band are **52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, and 144**. Check the **UNII-2 52-144** check box to include all channels, or check an individual check box.
 - **UNII-3 149-165**: The channels available for UNII-3 band are **149, 153, 157, 161, and 165**. Check the **UNII-3 149-165** check box to include all channels, or check an individual check box.
- f) Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **6, 9, 12, 18, 24, 36, 48, and 54**.
- g) Under **Mandatory Data Rates**, check the check boxes next to the individual data rates. You can choose up to two data rates. The available data rates are **6, 9, 12, 18, 24, 36, 48, and 54**.

The available data rates change depending on the data rates set under **Supported Data Rate**.

- h) Under **Tx Power Configuration**, set the power level and power threshold for an AP.
- **Power Level**: Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm to 30 dBm and the default is -10 dBm.
 - **TPC Power Threshold**: Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
 - **RX SOP**: Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an AP's radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High, Medium, Low, or Auto** threshold values for each 802.11 band.

- i) Under **Coverage Hole Detection**, configure the following:

Note You must enable global coverage hole detection in **Tools > Model Config Editor > Wireless > RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see [Create a Model Config Design for RRM General Parameters, on page 329](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
 - In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
 - In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
 - In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.
- j) In the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note Maximum client limit is not supported on the Cisco AireOS Wireless Controller.

- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

k) Under **Flexible Radio Assignment (FRA)**, check the **Client Aware** check box to enable the Client Aware feature.

This feature monitors the dedicated 5-GHz radio and when the client load passes the threshold, automatically changes the FRA from a monitor role into a 5-GHz role, effectively doubling the capacity of the cell on demand. Once the capacity crisis is over and Wi-Fi load returns to normal, the radios resume their previous roles.

Note You must enable FRA in **Tools > Model Config Editor > Wireless > RRM FRA Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM FRA parameters, see [Create a Model Config Design for RRM FRA Parameters, on page 328](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

If you enable the Client Aware feature, configure the following:

- In the **Client Select (%)** field, enter a value for client selection. The valid range is from 0 through 100 percent. The default value is 50 percent.
- In the **Client Reset (%)** field, enter a reset value for the client. The valid range is from 0 through 100 percent. The default value is 5 percent.

l) Under **802.11ax**, configure the following spatial reuse parameters:

Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 8 Configure the following in the **6 GHz** tab:

a) Ensure that the **6 GHz** toggle button is enabled.

- Note**
- 6-GHz radio is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
 - For Cisco Catalyst 9800 Series Wireless Controller, if you disable the **6 GHz** toggle button, Cisco DNA Center disables the Admin status of the **6 GHz** RF profile.

- b) Enable the **Enable PSC Enforcing** toggle button to allow Preferred Scanning Channel (PSC) enforcement. PSC enforcement improves the connectivity of the 6-GHz devices by prioritizing the PSC-enabled channels.

Note If you enable PSC enforcement, the check boxes next to the non-PSC channels are dimmed.

- c) Under **DCA Channel**, configure the following to manage channel assignments.
- Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.
 - **UNII-5 1-93**
 - **UNII-6 97-113**
 - **UNII-7 117-185**
 - **UNII-8 189-233**
 - Click **Show Advanced** to select the channel numbers for each band.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- d) Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an access point and a client. The available data rates are **6, 9, 12, 18, 24, 36, 48, and 54**.
- e) Under **Mandatory Data Rates**, check the check boxes next to the individual data rates. You can choose up to two data rates. The available data rates are **6, 9, 12, 18, 24, 36, 48, and 54**.

The available data rates change depending on the data rates set under **Supported Data Rate**.

- f) Under **Tx Power Configuration**, set the power level and power threshold for an AP.
- **Power Level:** Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference with another AP on the same channel or in close proximity. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm to 30 dBm and the default is -10 dBm.
 - **TPC Power Threshold:** Is the cutoff signal level used by Radio Resource Management (RRM) to determine whether to reduce the power of an AP. Use the **Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm to 80 dBm and the default threshold is -70 dBm.
 - **RX SOP:** Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level in dBm at which an AP's radio demodulates and decodes a packet. From the RX SOP drop-down list, choose **High, Medium, Low, or Auto** threshold values for each 802.11 band.

- g) Under **Coverage Hole Detection**, configure the following:

Note You must enable global coverage hole detection in **Tools > Model Config Editor > Wireless > RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see [Create a Model Config Design for RRM General Parameters, on page 329](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

h) In the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note

- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7 or later and earlier than Cisco IOS XE Release 17.9, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9 or later, the maximum client limit is 500.

i) Under **Flexible Radio Assignment (FRA)**, complete the following:

Note

- You must enable FRA in **Tools > Model Config Editor > Wireless > RRM FRA Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM FRA parameters, see [Create a Model Config Design for RRM FRA Parameters, on page 328](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).
- FRA is supported only on wireless controllers that run Cisco IOS XE Release 17.9.1 and later.

- In the **Client Reset Count** field, enter a reset count value for the client. The valid range is from 0 through 10. The default value is 1.
- In the **Client Utilization Threshold (%)** field, enter a utilization threshold value for the client. The valid range is from 0 through 100 percent. The default value is 5 percent.

j) Under **802.11ax**, configure the following multiple basic service set identifier (BSSID) and spatial reuse parameters:

- From the **6 GHz Discovery Frames** drop-down list, choose the required option from **None**, **Broadcast Probe Response**, and **FILS Discovery**.
6-GHz discovery frames are needed if the 6-GHz radio is the only operational radio. For more information about the 6-GHz discovery frames, click **Learn More**.
- In the **Broadcast Probe Response Interval (msec)** field, enter the broadcast probe response interval, in msec. The valid range is from 5 msec through 25 msec. The default value is 20 msec.

- Under **MULTI BSSID**, check the check boxes to enable the following parameters:
 - Downlink OFDMA
 - Uplink OFDMA
 - Downlink MU-MIMO
 - Uplink MU-MIMO
 - Target wake time
 - TWT Broadcast Support

Note You must enable multiple BSSID in **Tools > Model Config Editor > Wireless > Dot11ax Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for Dot11ax, see [Create a Model Config Design for Dot11ax Configuration, on page 321](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 9 Click **Save**.

Step 10 To mark a profile as the default RF profile, check the **Profile Name** check box and click **Mark Default**.

Step 11 In the **Warning** window, click **OK**.

What to do next

You must provision the APs to apply the RF profile settings on the device. For more information, see [Provision a Cisco AP—Day 1 AP Provisioning, on page 397](#).

Edit or Delete a Basic Radio Frequency Profile

The following procedure describes how to edit or delete a basic RF profile.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **Wireless Radio Frequency Profile** area, click the **Basic RF Profile** tab.

Note The **Basic RF Profile** table lists the number of created basic RF profiles based on **Profile Name**, **Type**, **2.4 GHz Data Rates**, **5 GHz Data Rates**, **6 GHz Data Rates**, **Channel Width**, and **Profile Type**.

Step 5 Check the check box next to the basic profile name that you want to edit.

Step 6 From the **Action** drop-down list, choose **Edit/View**.

Note You can edit one basic RF profile at a time.

Step 7 In the **Edit Wireless Radio Frequency Profile** window, configure the basic RF profile settings. For more information, see [Create a Wireless Radio Frequency Profile, on page 227](#).

Step 8 Click **Save**.

Step 9 To delete a basic RF profile, check the check box next to the basic RF profile name.

Step 10 From the **Action** drop-down list, choose **Delete** and then click **Yes**.

Step 11 To mark a basic RF profile as the default, check the check box next to a basic RF profile name.


Step 12 From the **Action** drop-down list, choose **Mark Default** and then click **Yes**.

What to do next

For Cisco AireOS Wireless Controllers, if you modify the DCA channels or data rates for an RF profile that is already provisioned on a wireless controller, Cisco DNA Center resets the corresponding radio.

If you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovision also pushes the RF profile updates to the devices and reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see [Provision a Cisco AireOS Controller, on page 391](#) and [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).

Prerequisites for Configuring AI Radio Frequency Profiles

- You must enable Cisco AI Network Analytics under the system settings. For more information, see [Configure Cisco AI Network Analytics Data Collection in Cisco DNA Center Administrator Guide](#).
- You must enable **AI-Enhanced RRM** under **Cisco AI Analytics** in the system settings. Click the menu icon () and choose **System > Settings > External Services > Cisco AI Analytics**.
In the **Cisco AI Analytics** window, under the **AI-ENHANCED RRM** area, click the toggle button to enable the AI-Enhanced RRM.
- Cisco AI RF profiles are supported only on Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE Release 17.7.1 or later.



Note Ensure that the **Group Mode** option for all the three bands (2.4 GHz, 5 GHz, and 6 GHz) is configured as **auto** or **leader** on the wireless controller.

- Cisco AI RF profiles are supported for 6-GHz radio only on wireless controllers that run Cisco IOS XE Release 17.9.1 and later.
- You must be a **Super Admin** or **Network Admin**.

Create an AI Radio Frequency Profile

The following procedure describes how to create an AI radio frequency profile for your building.

Before you begin

Ensure that the prerequisites are met. For more information, see [Prerequisites for Configuring AI Radio Frequency Profiles](#), on page 236.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **Wireless Radio Frequency Profile** area, hover your cursor over **Add** and choose **AI RF Profile**.

Step 5 In the **Profile Name** field of the **Create AI Radio Frequency Profile** window, enter the RF profile name.

Step 6 In the **Radio Frequency Settings** area of **Basic Settings**, check the **2.4 GHz**, **5 GHz**, or **6 GHz** check box.

The radio frequencies are checked by default. If you uncheck a radio frequency, Cisco DNA Center disables the Admin status of the corresponding RF profile.

Note Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS XE Release 17.9.1 and later support the AI RF profile for the **6 GHz** radio band.

Step 7 In the **Busy Hours** area, define the start and end time of the site time zone.

Note Busy hours are dependent upon the time zone of the building. You must configure a timezone under network settings for the respective building.

Step 8 In the **Busy Hour Sensitivity** area, click the **Low**, **Medium**, or **High** radio button to define the threshold of Radio Resource Management (RRM) sensitivity for the busy hours interval.

Step 9 In the **Enable RF Settings** area, click the toggle buttons under the **2.4 GHz**, **5 GHz**, or **6 GHz** columns to enable or disable RF settings for the corresponding radio bands.

The supported RF settings are:

- **Flexible Radio Assignment (FRA)**: FRA optimizes the radio coverage per band and determines the best role assignment for redundant radios.
- **Dynamic Channel Assignment (DCA)**: DCA dynamically manages channel assignment for an RF group and evaluates the assignments on a per-AP radio basis.
- **Transmit Power Control (TPC)**: TPC manages and transmits power for APs. It also maximizes the SNR during the reduction in interference.
- **Dynamic Bandwidth Selection (DBS)**: DBS monitors and adjusts the channel width to balance the performance and interference.

- Note**
- When you disable the **2.4 GHz** radio band for FRA, it automatically disables the **5 GHz** radio band for FRA, and conversely.
 - When you disable the **5 GHz** radio band for DCA, it disables the **2.4 GHz** radio band for FRA and the **5 GHz** radio band for FRA and DBS.
 - You can individually enable the **2.4 GHz** radio band for DCA and TPC; and the **5 GHz** radio band for DCA, TPC, and DBS. For the **5 GHz** radio band, if DCA and DBS are disabled and you enable DBS, DCA is also enabled.
 - You can enable or disable the **6 GHz** radio band together for DCA and DBS RF settings. You can individually enable the **6 GHz** radio band for TPC.
 - FRA is not supported for the **6 GHz** radio band.

Step 10 Expand **Advanced** and click the **2.4 GHz** toggle button.

- a) In the **DCA Channel** area, check the **Select All** check box to select DCA channels **1, 6, and 11**. Alternatively, check the individual check boxes next to the channel numbers.
- b) In the **Advanced Options** area, check the **Select All** check box to select all the DCA channels.
- c) Click **Show Advanced** to select the remaining channel numbers.
- d) Check the check box next to the individual channel numbers. The channel numbers that are available for the profile are **2, 3, 4, 5, 7, 8, 9, 10, 12, 13, and 14**.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- e) In the **Supported Data Rate** area, configure the following:
 - Check the **Enable 802.11b data rates** check box to enable the 802.11b data rates. This action also enables the 802.11b supported data rate check boxes in the **Mandatory Data Rates** area.
 - Use the slider to set the rates at which data can be transmitted between an AP and a client. The available data rates are **1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54**.
- f) In the **Mandatory Data Rates** area, check the check box next to the individual data rates. You can choose up to two data rates. The available data rates are **1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54**.
- g) In the **Tx Power Configuration** area, set the following:
 - **Power Level:** Determines whether the power of an AP needs to be reduced. Reducing the power of an AP helps mitigate co-channel interference. Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm through 30 dBm. The minimum default is -10 dBm and maximum default is 30 dBm.
 - **TPC Power Threshold:** Is the cutoff signal level used by RRM to determine whether to reduce the power of an AP. Use the **TPC Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm through 80 dBm and the default threshold is -70 dBm.
 - **RX SOP:** Receiver Start of Packet Detection Threshold (RX SOP) determines the Wi-Fi signal level, in dBm, at which an AP's radio demodulates and decodes a packet. From the **RX SOP** drop-down list, choose **High, Medium, Low, or Auto** threshold values for each 802.11 band.

h) Under **Coverage Hole Detection**, configure the following:

Note You must enable global coverage hole detection in **Tools > Model Config Editor > Wireless > RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see [Create a Model Config Design for RRM General Parameters, on page 329](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

i) In the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

Note

- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.
- If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.
- If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

j) Under **802.11ax**, configure the following spatial reuse parameters:

Note 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 11 In the **Advanced** area, click the **5 GHz** toggle button.

a) Check the **Zero Wait DFS** check box to allow APs with 5-GHz radio to switch to a new channel without any waiting time.

Note Cisco DNA Center supports Zero wait DFS for Cisco Wireless Controllers running Cisco IOS XE Release 17.9.1 and later.

- b) Use the **DBS Max Width** slider to set the channel width of the AI RF profile.

The available channel width options are **20 MHz, 40 MHz, 80 MHz, or 160 MHz**.

The **Auto Channels Logic** area displays a color-coded representation of channels that are available in the Unlicensed National Information Infrastructure (UNII) radio bands for the available channel widths.

You can select **DBS Max Width** only when DBS is enabled.

When you disable the DBS, Cisco DNA Center allows you to select the static channel width.

- c) Set the **DCA Channel** to manage the following channel assignments:

- **UNII-1 36-48**: The channels available for UNII-1 band are **36, 40, 44, and 48**.
- **UNII-2 52-144**: The channels available for UNII-2 band are **52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, and 144**.
- **UNII-3 149-165**: The channels available for UNII-3 band are **149, 153, 157, 161, and 165**.

- d) Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.

- e) Click **Show Advanced** to view and select the individual DCA channel numbers.

- Check the **UNII-1 36-48** check box to include all channels, or check an individual check box.
- Check the **UNII-2 52-144** check box to include all channels, or check an individual check box.
- Check the **UNII-3 149-165** check box to include all channels, or check an individual check box.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- f) Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an AP and a client. The available data rates are **6, 9, 11, 12, 18, 24, 36, 48, and 54**.

- g) In the **Mandatory Data Rates** area, check the check box next to the individual data rates. You can choose up to two data rates. The available data rates are **6, 9, 11, 12, 18, 24, 36, 48, and 54**.

- h) In the **Tx Power Configuration** area, set the **Power Level, Power Threshold, and RX SOP**.

- Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm through 30 dBm. The minimum default is -10 dBm and maximum default is 30 dBm.
- Use the **TPC Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm through 80 dBm and the default threshold is -70 dBm.
- From the **RX SOP** drop-down list, choose **High, Medium, Low, or Auto** threshold values.

- i) Under **Coverage Hole Detection**, configure the following:

Note You must enable global coverage hole detection in **Tools > Model Config Editor > Wireless > RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see [Create a Model Config Design for RRM General Parameters, on page 329](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

j) In the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

- Note**
- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.
 - If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.
 - If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

k) Under **802.11ax**, configure the following spatial reuse parameters:

- Note** 802.11ax is supported only on wireless controllers that run Cisco IOS XE Release 17.6.1 and later.
- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
 - In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
 - Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
 - In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
 - In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 12 In the **Advanced** area, click the **6 GHz** toggle button.

a) Use the **DBS Width** slider to set the minimum and maximum channel width of the AI RF profile.

The available channel width options are **20 MHz**, **40 MHz**, **80 MHz**, or **160 MHz**.

The **Auto Channels Logic** area displays a color-coded representation of channels that are available in the UNII radio bands for the available channel widths.

You can select **DBS Width** only when DBS is enabled.

- b) Enable the **Enable PSC Enforcing** toggle button to allow Preferred Scanning Channel (PSC) enforcement.

PSC enforcement improves the connectivity of the 6-GHz devices by prioritizing the PSC-enabled channels.

Note If you enable PSC enforcement, the check boxes next to the non-PSC channels are dimmed and the check boxes next to the PSC channels are checked by default. If necessary, you can uncheck the check box next to the required PSC channel.

- c) Set the **DCA Channel** to manage the following channel assignments:

- **UNII-5 1-93**: The channels available for the UNII-5 band are **1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, and 93**.
- **UNII-6 97-113**: The channels available for the UNII-6 band are **97, 101, 105, 109, and 113**.
- **UNII-7 117-185**: The channels available for the UNII-7 band are **117, 121, 125, 129, 133, 137, 141, 145, 149, 153, 157, 161, 165, 169, 173, 177, 181, and 185**.
- **UNII-8 189-233**: The channels available for the UNII-8 band are **189, 193, 197, 201, 205, 209, 213, 217, 221, 225, 229, and 233**.

- d) Check the **Select All** check box to include all DCA channels, or check an individual check box to select an individual DCA channel.

- e) Click **Show Advanced** to select the remaining DCA channel numbers.

- Check the **UNII-5 1-93** check box to include all channels, or check an individual check box.
- Check the **UNII-7 117-185** check box to include all channels, or check an individual check box.
- Check the **UNII-8 189-233** check box to include all channels, or check an individual check box.

Note Select the DCA channels based on the country code of the device. During provisioning, only the allowed channels for the country configured on the wireless controller are considered and the unsupported channels are ignored. Provisioning may fail if all the channels that you've selected are unsupported as per the country codes configured on the controller.

- f) Use the **Supported Data Rate** slider to set the rates at which data can be transmitted between an AP and a client. The available data rates are **6, 9, 12, 18, 24, 36, 48, and 54**.

- g) In the **Tx Power Configuration** area, set the **Power Level**, **TPC Power Threshold**, and **RX SOP**.

- Use the **Power Level** slider to set the minimum and maximum power level. The range is from -10 dBm through 30 dBm and the default is -10 dBm.
- Use the **TPC Power Threshold** slider to increase and decrease the power value, which causes the AP to operate at higher or lower transmit power rates. The range is from -50 dBm through 80 dBm and the default threshold is -70 dBm.
- From the **RX SOP** drop-down list, choose **High**, **Medium**, **Low**, or **Auto** threshold values.

- h) Under **Coverage Hole Detection**, configure the following:

Note You must enable global coverage hole detection in **Tools > Model Config Editor > Wireless > RRM General Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for RRM general parameters, see [Create a Model Config Design for RRM General Parameters, on page 329](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

- In the **Minimum Client Level (clients)** field, enter a value for the minimum number of clients. The valid range is from 1 through 200. The default value is 3.
- In the **Data RSSI Threshold (dBm)** field, enter the data Received Signal Strength Indication (RSSI) threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Voice RSSI Threshold (dBm)** field, enter the voice RSSI threshold in dBm. The valid range is from -90 dBm through -60 dBm. The default value is -80 dBm.
- In the **Exception Level (%)** field, enter an exception level. The valid range is from 0 through 100 percent. The default value is 25 percent.

i) In the **Max Clients** field, enter the maximum client limit value. The valid range is from 0 through 500.

- Note**
- If the wireless controller is running a version earlier than Cisco IOS XE Release 17.7.1, the maximum client limit is 200.
 - If the wireless controller is running Cisco IOS XE Release 17.7.1 or later and earlier than Cisco IOS XE Release 17.9.1, the maximum client limit is 400.
 - If the wireless controller is running Cisco IOS XE Release 17.9.1 or later, the maximum client limit is 500.

j) Under **802.11ax**, configure the following multiple basic service set identifier (BSSID) and spatial reuse parameters:

- From the **6 GHz Discovery Frames** drop-down list, choose the required option from **None**, **Broadcast Probe Response**, and **FILS Discovery**.

6-GHz discovery frames are needed if the **6 GHz** radio is the only operational radio. For more information about the 6-GHz discovery frames, click **Learn More**.

- In the **Broadcast Probe Response Interval (msec)** field, enter the broadcast probe response interval, in msec. The valid range is from 5 msec through 25 msec. The default value is 20 msec.
- Under **MULTI BSSID**, check the check boxes to enable the following parameters:
 - Downlink OFDMA
 - Uplink OFDMA
 - Downlink MU-MIMO
 - Uplink MU-MIMO
 - Target wake time
 - TWT Broadcast Support

Note You must enable multiple BSSID in **Tools > Model Config Editor > Wireless > Dot11ax Configuration** for the corresponding radio band and provision it on the managing wireless controller. For more information about the model configuration design for Dot11ax, see [Create a Model Config Design for Dot11ax Configuration, on page 321](#). For more information about provisioning, see [Provision Wireless Devices, on page 389](#).

- Check the **OBSS PD** check box to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- In the **Non-SRG OBSS PD Max Threshold (dBm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.
- Check the **SRG OBSS PD** check box to enable the SRG OBSS-PD functionality.
SRG OBSS-PD is supported only on wireless controllers that run Cisco IOS XE Release 17.7.1 and later.
- In the **SRG OBSS PD Min Threshold (dBm)** field, enter a value for the SRG OBSS-PD minimum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -82 dBm.
- In the **SRG OBSS PD Max Threshold (dBm)** field, enter a value for the SRG OBSS-PD maximum threshold, in dBm. The valid range is from -82 dBm through -62 dBm. The default value is -62 dBm.

Step 13 Click **Save**.

What to do next

You must provision the APs to apply the RF profile settings on the device. For more information, see [Provision a Cisco AP—Day 1 AP Provisioning, on page 397](#).

Edit an AI Radio Frequency Profile

The following procedure describes how to edit an AI RF profile.

Before you begin

Ensure that the prerequisites are met. For more information, see [Prerequisites for Configuring AI Radio Frequency Profiles, on page 236](#).

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.

The **AI RF Profile** table lists the number of created AI RF profiles based on **Profile Name**, **Busy Hours**, **Busy Hour Sensitivity**, **FRA**, **DCA**, **DBS**, **TPC**, and **Mapped Buildings**.

Step 5 Check the check box next to the AI RF profile that you want to edit.

You can edit one AI RF profile at a time.

Step 6 Click **Edit/View**.

- Step 7** In the **Edit AI RF Profile** window, configure the AI RF profile settings. For more information, see [Create an AI Radio Frequency Profile, on page 237](#).
- Step 8** Click **Save**.

What to do next

If you update an RF profile that is already provisioned on a wireless controller and AP, you must reprovision either the wireless controller or AP. Wireless controller reprovision also pushes the RF profiles updates to the devices and reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).

Delete an AI Radio Frequency Profile

The following procedure describes how to delete an AI RF profile.

Before you begin

Ensure that the prerequisites are met. For more information, see [Prerequisites for Configuring AI Radio Frequency Profiles, on page 236](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.
- The **AI RF Profile** table lists the number of created AI RF profiles based on **Profile Name**, **Busy Hours**, **Busy Hour Sensitivity**, **FRA**, **DCA**, **DBS**, **TPC**, and **Mapped Buildings**.
- Step 5** To delete an AI RF profile, check the check box next to the AI RF profile that you want to delete.
- Step 6** Click **Delete** and then click **Yes**.
- Note** Cisco DNA Center does not allow you to delete an AI RF Profile which is already assigned to a building.

What to do next

If you delete an RF profile that is already provisioned on a wireless controller and AP, you must reprovision the wireless controller. Reprovisioning the AP is not necessary. For more information about provisioning a wireless controller, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).

Configure an AI Radio Frequency Profile

The following procedure describes how to assign an AI RF profile to a building.

Before you begin

Ensure that the prerequisites are met. For more information, see [Prerequisites for Configuring AI Radio Frequency Profiles, on page 236](#).

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure AI RF Profile**.
- Step 2** In the **Assign AI RF Profiles** window, click **Let's Do it** to go directly to the workflow.
- Step 3** In the **Task Name** field of the **Configure AI RF Profile** window, enter a task name.
- Step 4** In the **Select Locations to Assign AI RF Profiles** window, select the locations where you want to assign the AI-enabled RF profiles. You can either search for a site by entering its name in the **Find Hierarchy** field, or expand **Global** and choose the sites.

The **Site selection summary** table lists the sites based on the site selection in the site hierarchy and displays the **Selected Location** and **Impacted Location** of the selected sites.

- **Selected Locations:** A location that is being enabled for AI RF profile.
- **Impacted Locations:** A location that is being partially managed by the same wireless controller of the selected location.

Note When a controller manages more than one building and if you enable the AI RF profile only on one building, Cisco DNA Center automatically enables other building with same AI RF profile.

For example, if two controllers manage three buildings and you enable AI RF profile on one building, Cisco DNA Center automatically enables other two buildings with the same AI RF profile.

- Step 5** In the **Select AI RF Profiles to assign** window, the **Building** table lists AI RF profiles based on **Location**, **Floors**, **Current RF Profiles**, and **Replace with AI RF Profiles**.
- In the **Building** table, check the check box next to a location to choose an AI RF profile.
 - Based on the location, choose an AI-enabled RF profile from the drop-down list under **Replace with AI RF Profiles** to replace with the current AI RF profile.
 - If the AI RF profile is not created, click the three dots under the **Action** column to create a new AI RF profile, or copy the current RF profile and AI settings.
 - You can also create an AI RF profile from the **Create a new AI RF Profile to apply** link in the **Select AI RF Profiles to assign** window. For more information, see [Create an AI Radio Frequency Profile, on page 237](#).

- Step 6** In the **Details of selected AI RF Profile** window, review the **AI Settings**, **Common Settings**, and **Assignment** details of the AI-enabled RF profiles.

Note AI-enhanced RRM computation occurs every 30 minutes. RRM decisions are updated and pushed to devices after the computation.

- Step 7** In the **Summary** window, review the **Task Details**, **Select Locations to Assign AI RF Profiles**, and **Select AI RF Profiles to assign**.

- Step 8** In the **Deploy the AI RF Profiles** window, choose whether you want to deploy profiles **Now** or schedule it for later.

- Step 9** Click **Continue**.

The **Done! AI RF Profiles Assigned** window opens.

- Step 10** Click the menu icon (☰) and choose **Activities > Tasks**.

- Step 11** In the **Tasks** window, click the task link.

A slide-in pane displays the **Assigned Building(s)**, **Selected AI RF Profile**, and **Provision Details**.

Assign a Location to an Existing AI RF Profile

The following procedure describes how to assign a location to an existing AI RF profile.

Before you begin

Ensure that the prerequisites are met. For more information, see [Prerequisites for Configuring AI Radio Frequency Profiles](#), on page 236.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.
The **AI RF Profile** table lists the number of created AI RF profiles.
- Step 5** Click the three dots under the **Action** column for an AI RF profile.
- Step 6** From the drop-down list, choose **Assign Location**.
The **Manage Location Assignment** window opens.
- Step 7** You can either search for a site by entering its name in the **Search** field, or expand **All Sites** to choose the sites.
- Note**
- The site hierarchy shows the AI-enabled locations.
 - Sites or buildings that are not eligible for the AI profile are disabled.
 - You cannot select a floor under a building. When you select a building for an AI-enabled RF profile, the floors underneath are assigned automatically.
- If the same wireless controller manages other buildings, the **Confirm Impacted Sites** window opens.
- Step 8** Review the confirmation and click **Confirm** to assign the chosen sites to the AI-enabled RF profile.
- Step 9** Click **Assign**.
A **Download a Backup of Current RF Settings** window opens that allows you to download the backup of the RF settings across the selected buildings.
- Step 10** (Optional) Click the backup link to download a .csv file to your local machine.
- Step 11** Click **Confirm**.
- Step 12** In the subsequent confirmation window, click **Confirm**.
In the **AI RF Profile** table, the locations assigned to the AI RF profile are displayed under the **Mapped Buildings** column.
-

What to do next

Provision Devices of an AI RF Profile-Enabled Building

The following procedure describes how to provision devices across the locations to deploy the AI RF profile.

1. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

In the **Inventory** window, the **Device** table lists the discovered AI RF profile associated devices.

2. Check the check box next to the AI RF profile associated device name that you want to provision.
3. From the **Actions** drop-down list, choose **Provision > Provision Device**.
4. Proceed through all the steps and in the **Summary** step, click **Deploy**.
5. In the **Summary** window, view the remaining network settings that will be pushed to the device. For more information, see [Wireless Device Provisioning Overview, on page 389](#).

Unassign a Location from an Existing AI RF Profile

The following procedure describes how to unassign a location from an existing AI RF profile.

Before you begin

Ensure that the prerequisites are met. For more information, see [Prerequisites for Configuring AI Radio Frequency Profiles, on page 236](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** In the **Wireless Radio Frequency Profile** area, click the **AI RF Profile** tab.
The **AI RF Profile** table lists the number of created AI RF profiles.
- Step 5** Click the three dots under the **Action** column for an AI RF profile.
- Step 6** From the drop-down list, choose **Unassign Location**.
The **Unassign AI RF Profile** window opens.
- Step 7** Check the check box next to a site to unassign an AI RF profile.
- Step 8** Click the **Select from available RF Profiles** radio button to select an available RF profile that you want to assign to the chosen location.
- Step 9** From the **Select RF Profile to Replace** drop-down list, choose an RF profile.
The **Select RF Profile to Replace** drop-down list shows AI RF profiles and basic RF profiles.
If you select a basic RF profile from the drop-down list, a **Confirm Impacted Sites** window validates whether the same wireless controller manages the other site.
Review the **Confirm Impacted Sites** window and click **Confirm** to assign the chosen sites to the selected RF profile.
- Step 10** Click **Upload a CSV with RF settings back** to upload a backup of the RF settings from your local machine.
- Step 11** Click **Choose a file** to import the CSV file, or drag and drop the CSV file to the drag and drop area.
Note The maximum size of the CSV file is 10 MB.
From the uploaded CSV file, if you find an RF setting based on the selected location name, a **Confirm RF Settings for Selected Locations** window shows the **Location** and **Matched RF Profiles**.
- Step 12** Review the **Confirm RF Settings for Selected Locations** window and click **Confirm**.
- Step 13** Click **Unassign**.

- Step 14** In the confirmation window, click **Continue**.
- Step 15** Click the menu icon (☰) and choose **Activities > Tasks >** to view upcoming, in progress, completed, and failed unassign location to AI RF profile tasks.
-

What to do next

Provision Devices of an AI RF Profile-Enabled Building

The following procedure describes how to provision the devices across the AI RF profile assigned locations to deploy the AI RF profile.

1. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
In the **Inventory** window, the **Device** table lists the discovered AI RF profile associated devices.
2. Check the check box next to the AI RF profile associated device name that you want to provision.
3. From the **Actions** drop-down list, choose **Provision > Provision Device**.
4. Proceed through all the steps and in the **Summary** step, click **Deploy**.
5. In the **Summary** window, review the remaining network settings that will be pushed to the device. For more information, see [Wireless Device Provisioning Overview, on page 389](#).

Upgrade a Basic Radio Frequency Profile to an AI Radio Frequency Profile

Before you begin

Ensure that the prerequisites are met. For more information, see [Prerequisites for Configuring AI Radio Frequency Profiles, on page 236](#).

To onboard a site in an AI-enhanced RRM service, at least one of the following services must be enabled:

- Flexible Radio Assignment (FRA)
 - Dynamic Channel Assignment (DCA)
 - Transmit Power Control (TPC)
 - Dynamic Bandwidth Selection (DBS)
-

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** Check the check box next to the basic RF profile name that you want to upgrade to an AI RF profile.
- Step 5** From the **Action** drop-down list, choose **Upgrade to AI**.
- Step 6** In the confirmation window, click **Yes**.

Step 7 In the **Edit AI RF Profile** window, configure the AI RF profile settings. For more information, see [Create an AI Radio Frequency Profile](#), on page 237.

Create an AP Authorization List

Cisco DNA Center allows you to configure a list of authorized APs. Cisco DNA Center supports the following types of AP authorization:


- Local authorization: Uses the AP MAC address, serial number, or both, for authorization against the local database.
- AAA authorization: Uses a list of AAA servers for authorization.

You can choose the AP authorization list while provisioning the Cisco Wireless Controller. Cisco Wireless Controllers respond only to requests from the APs that are present in the AP authorization list.



Note

- If both MAC address and serial number are required for an AP authorization, ensure that both are added to the AP authorization list. If one of these AP entries isn't available in the AP authorization list provisioned for a wireless controller, the corresponding AP can't join the network.
- For mesh AP (MAP), you must add the MAC address for AP authorization.
- For Cisco AireOS Wireless Controllers, Cisco DNA Center supports only the MAC address for AP authorization. If you configure both MAC address and serial numbers, only MAC address is used for Cisco AireOS Wireless Controllers.
- For Cisco Catalyst 9800 Series Wireless Controllers, Cisco DNA Center supports the configuration of AP authorization lists only on the wireless controllers running Cisco IOS Release 17.5 and later.

Step 1 Click the menu icon () and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **AP Authorization List** table, click **Add**.

Step 5 In the **AP Authorization List** slide-in pane, enter a name for the AP authorization list.

Step 6 To configure local authorization, do the following:

- In the **Local Auth** tab, check the **Configure Local Authorization** check box.
- In the **Type** area, choose an authorization type:
 - To use the AP MAC address for authorization, click **Mac Address**.
 - To use the AP serial number for authorization, click **Serial Number**.
- To enter the AP MAC address or serial number data, do one of the following:
 - To add the MAC address or serial number individually to the authorization list, click **Add**. In the **AP Entry** field, enter the data.

- To upload the CSV file with the data, click **Upload**. In the dialog box, do the following:
 1. Drag and drop your CSV file into the drag and drop area. Alternatively, click **Choose a file** and browse to select your CSV file stored locally.
 - Note** If you don't have a CSV file, click **Download** to download a CSV file that you can edit and upload.
 2. Click **Save**.
- d) (Optional) To use both the MAC address and serial number for authorization:
 1. Click **Mac Address** and enter the AP MAC address data (6.c, on page 250).
 2. Click **Serial Number** and enter the AP serial number data (6.c, on page 250).

Step 7 To configure AAA authorization, do the following:

- a) In the **AAA Auth** tab, check the **Configure AAA Authorization** check box.
- b) Based on the AP authorization requirement for the AAA server, do one of the following:
 - If the AAA server uses only the MAC address for AP authorization, check the **Authorize AP against MAC Address** check box.
 - If the AAA server uses only the serial number for AP authorization, check the **Authorize AP against Serial Number** check box.
 - If the AAA server uses both the MAC address and serial number for AP authentication, check both the **Authorize AP against MAC Address** and **Authorize AP against Serial Number** check boxes.
- c) To add AP entries to the AP authorization list, do one of the following:
 - Click the plus icon (+) next to the required AP entry.
 - Click the AP entry and click **Add Selected**.
 - Note** To choose multiple AP entries, press **Shift**, click the AP entries, and click **Add Selected**.
 - To add all the AP entries to the AP authorization list, click **Add All**. You can use the **Search** field to filter the AP entries.

Step 8 Click **Save**.

Edit or Delete an AP Authorization List

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** In the **AP Authorization List** table, check the check box next to the authorization list name that you want to edit or delete.

- To edit the AP authorization list, click **Edit**. In the **AP Authorization List** slide-in pane, edit the configuration as necessary, and click **Save**. For more information, see [Create an AP Authorization List, on page 250](#).
- To delete the AP authorization list, click **Delete**, and then click **Yes**.

Create an Anchor Group

You can create anchor groups with up to three Cisco Wireless Controllers and set the priority for the anchors. You can add the following devices as anchors:

- Cisco Wireless Controllers that are managed by Cisco DNA Center.
- Cisco Wireless Controllers that are not managed by Cisco DNA Center (external wireless controllers).



Note You must add at least one anchor to an anchor group.

Priority order of the anchors determines the traffic sharing across the anchors:

- Equal sharing: When the priority order of all the anchors is the same (for example, 1, 1, and 1).
- Partial sharing: When the priority order of more than one anchor is the same (for example, 1, 1, and 2).
- Sequential sharing: When the priority order of the anchors is sequential (for example, 1, 2, and 3).

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **Anchor Group** table, click **Add**.

Step 5 In the **Anchor Group Name** field of the **Anchor Group** slide-in pane, enter the anchor group name.

Step 6 To add a managed wireless controller as an anchor, click **Add Managed WLC** and do the following in the **Add Managed WLC** dialog box:

- a) Check the check box next to the name of the devices that you want to add as anchors.

To search for a device, in the **Search Table** search field, enter either the partial name or the full name of the device and press **Enter**.

- b) Click **Add**.

Step 7 (Optional) To add an external wireless controller as an anchor, click **Add External WLC** and do the following in the **Add External WLC** dialog box:

- a) In the **Device Name** field, enter the device name.
- b) From the **Device Series** drop-down list, choose a device series.
- c) In the **Peer IP Address** field, enter the peer IP address.
- d) (Optional) In the **NAT IP Address** field, enter the Network Address Translation (NAT) IP address.
- e) In the **MAC Address** field, enter the MAC address of the device.
- f) In the **Mobility Group Name** field, enter the mobility group name.

g) (Optional) In the **Hash** field, enter the hash for the Cisco Catalyst 9800 Series Wireless Controller.

Note This field is available for only the Cisco Catalyst 9800-CL Wireless Controllers.

h) Click **Add**.

Step 8 (Optional) To add an existing external wireless controller as an anchor, click **Add Existing External WLC** and do the following in the **Add Existing External WLC** dialog box:

a) Check the check box next to the name of the devices that you want to add as anchors.

To search for a device, in the **Search Table** search field, enter either the partial name or the full name of the device and press **Enter**.

b) Click **Add**.

Step 9 (Optional) To set the priority for an anchor, from the **Priority Order** drop-down list, choose the priority for the anchor wireless controller.

Step 10 Click **Save**.

Edit or Delete an Anchor Group

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **Anchor Group** table, check the check box next to the anchor group that you want to edit or delete.

- To edit the anchor group, click **Edit**. In the **Anchor Group** slide-in pane, configure the anchors and click **Save**. For more information, see [Create an Anchor Group, on page 252](#).
 - To delete the anchor group, click **Delete** and then click **Yes**.
-

AP Profiles

AP profiles consolidate the AP authentication settings for Plug and Play (PnP), Cisco Advanced Wireless Intrusion Prevention System (aWIPS), rogue management, and mesh networks. AP profiles allow you to manage and provision APs.

Cisco DNA Center provides a default AP profile for Cisco IOS XE devices and Cisco AireOS devices. You can edit the default AP profiles, but you can't delete them. Site tags and AP groups generated by Cisco DNA Center use the default AP profiles.



Note When you upgrade to Release 2.3.5.5 from an earlier version, by default, Cisco DNA Center doesn't push the default AP profile to the wireless controller. To update the default AP profile on the wireless controller, you must explicitly save it on the **AP Profiles** window. For more information, see [Edit or Delete an AP Profile, on page 262](#).

When you save the default AP profile, if there's a difference between the current wireless controller configuration and the AP profile configuration saved on Cisco DNA Center, Cisco DNA Center pushes the default AP profile to the wireless controller during subsequent reprovisioning.

After saving the default AP profile, there's no option to prevent Cisco DNA Center from pushing the default AP profile to the wireless controller during reprovisioning.

You can also create custom AP profiles for Cisco IOS XE and Cisco AireOS devices. To assign an AP profile to a site, associate it with a wireless network profile.

Create an AP Profile for Cisco IOS XE Devices

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **AP Profile** table, hover your cursor over **Add** and choose **AP Profile for IOS-XE**.

Step 5 In the **Create Access Point Profile** window, enter a name for the AP profile.

Step 6 (Optional) Enter a description for the AP profile.

Step 7 If this AP profile is for remote teleworker APs or Cisco OfficeExtend APs, check the **Remote Teleworker** check box.

You can enable or disable the **Remote Teleworker** check box only while creating the AP profile. You can't update this option for existing AP profiles.

Note Remote teleworker-enabled AP profiles don't support the following settings:

- aWIPS application
- Rogue detection
- Mesh
- Power

Step 8 Configure the required settings in the followings tabs:

- a) **Management**: For more information, see [Configure Management Settings for an AP Profile for Cisco IOS XE Devices, on page 255](#).
- b) **Security**: For more information, see [Configure Security Settings for an AP Profile for Cisco IOS XE Devices, on page 256](#).
- c) **Mesh**: For more information, see [Configure Mesh Settings for an AP Profile for Cisco IOS XE Devices, on page 256](#).
- d) **Power**: For more information, see [Configure Power Settings for an AP Profile for Cisco IOS XE Devices, on page 258](#).
- e) **Additional**: For more information, see [Configure Additional Settings for an AP Profile for Cisco IOS XE Devices, on page 259](#).

Step 9 Click **Save**.

Configure Management Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the following for an AP profile for Cisco IOS XE devices:

- Authentication settings to onboard APs securely during the PnP claim process. Based on the authentication settings configured at the global-level or site-level hierarchy in Cisco DNA Center, PnP pushes the 802.1x (Dot1x) supplicant and certificates when claiming an AP. The AP uses the 802.1x supplicant for authenticating with Cisco ISE.
 - Authentication settings for day *n* authentication of APs.
 - Credentials for console access, SSH, and Telnet.
 - Enabling Cisco Discovery Protocol (CDP) to make an AP discoverable to its neighboring devices.
-

Step 1 In the **Create Access Point Profile** window (**Design > Network Settings > Wireless > AP Profile** table > **Add > AP Profile for IOS-XE**), click the **Management** tab.

Step 2 In the **Access Points Authentication** area, choose an authentication method.

Note This authentication method is used during the AP PnP claim and day *n* authentication. Changing the authentication method impacts the service of the APs onboarded through the PnP claim process. If you change the authentication method, perform a factory reset for the APs onboarded through PnP claim process. If an AP joins with a different Extensible Authentication Protocol (EAP) method, the EAP method changes based on the authentication method that you choose.

The following authentication methods are available:

- **NO-AUTH**: Default authentication method.
- **EAP-TLS**: EAP-Transport Level Security (EAP-TLS) uses certificate-based authentication.
- **EAP-PEAP**: EAP-Protected Extensible Authentication Protocol (EAP-PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. EAP-PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol.

If you choose **EAP-PEAP**, enter a username and password. Cisco DNA Center generates a certificate and applies it during the PnP claim process.

- **EAP-FAST**: EAP-Flexible Authentication through Secure Tunneling (EAP-FAST) provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.

If you choose **EAP-FAST**, enter a username and password. Cisco DNA Center generates a certificate and applies it during the PnP claim process.

Step 3 In the **SSH and Telnet** area, configure the following:

- a) (Optional) Click the **SSH** toggle button to configure the credentials for SSH.
- b) (Optional) Click the **Telnet** toggle button to configure the credentials for Telnet.
- c) In the **Username** field, enter the name used to authenticate the device.

Username can't contain spaces or angle brackets (<>).

Note If you disable SSH and Telnet, the **Username** field is optional.

d) In the **Password** field, enter the password used to authenticate the device.

Note If you disable SSH and Telnet, the **Password** field is optional.

e) In the **Enable Password** field, enter the password to enable a higher privilege level in the CLI.

Note If you disable SSH and Telnet, the **Enable Password** field is optional.

Step 4 In the **Cisco Discovery Protocol (CDP) State** area, click the **CDP State** toggle button to enable or disable CDP.

What to do next

Configure the other necessary settings for the AP profile. For more information, see [Create an AP Profile for Cisco IOS XE Devices, on page 254](#).

Configure Security Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the following for an AP profile for Cisco IOS XE devices:

- Cisco Advanced Wireless Intrusion Prevention System (aWIPS) and forensic capture to detect intrusion threats and mitigate them. Cisco DNA Center supports aWIPS for devices running Cisco IOS XE Release 17.3.1 or later.
- Rogue detection to detect the APs that are installed on the network without explicit authorization from a system administrator. Cisco DNA Center supports rogue detection for devices running Cisco IOS XE Release 17.4 or later.

Step 1 In the **Create Access Point Profile** window (**Design > Network Settings > Wireless > AP Profile** table > **Add > AP Profile for IOS-XE**), click the **Security** tab.

Step 2 In the **aWIPS and Forensic Capture Enablement** area, configure the following:

- Click the **aWIPS** toggle button to enable or disable aWIPS.
- Click the **Forensic Capture Enablement** toggle button to enable or disable forensic capture.

Note You must enable the **aWIPS** toggle button to use the **Forensic Capture Enablement** toggle button.

Step 3 In the **Rogue Detection** area, click the **Rogue Detection** toggle button to enable or disable rogue detection.

What to do next

Configure the other necessary settings for the AP profile. For more information, see [Create an AP Profile for Cisco IOS XE Devices, on page 254](#).

Configure Mesh Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the mesh settings for an AP profile for Cisco IOS XE devices.

Before you begin

Ensure that you add the MAC address of the mesh access point (MAP) to the AP authorization list. For more information, see [Create an AP Authorization List, on page 250](#).

-
- Step 1** In the **Create Access Point Profile** window (**Design > Network Settings > Wireless > AP Profile table > Add > AP Profile for IOS-XE**), click the **Mesh** tab.
- Step 2** Click the **Mesh** toggle button.
- Note** If you disable the **Mesh** toggle button, the existing custom mesh settings are deleted, and the AP profile is associated with the default mesh profile on the device.
- Step 3** (Optional) In the **Range - Root AP to Mesh AP (in feet)** field, enter the maximum range (in feet) from the root access points (RAP) to the MAPs in the network. The valid range is from 150 feet through 132000 feet.
- Step 4** (Optional) To allow wireless client association over the backhaul radio, check the **Backhaul Client Access** check box.
- Generally, the backhaul radio is a 5-GHz radio for most of the MAPs. The backhaul radio can carry both backhaul traffic and client traffic.
- If you disable the **Backhaul Client Access** check box, Cisco DNA Center sends only backhaul traffic over the backhaul radio, and client association is only over the secondary radio or radios.
- Step 5** (Optional) In the **RAP Downlink Backhaul** area, choose the required option.
- If your country prohibits the use of **5 GHz**, choose **2.4 GHz**. Even if your country allows the use of **5 GHz**, consider using **2.4 GHz** because 2.4-GHz radio can cover larger mesh or bridge distances.
- Note** When you change the RAP configuration from **5 GHz** to **2.4 GHz**, Cisco DNA Center propagates the update from the RAP to all the MAPs. At this point, the MAPs disconnect from the 5-GHz network and connect to the 2.4-GHz network.
- Step 6** (Optional) In the **Backhaul Data Rates** area, from the **5GHz Band Radio Type** and **2.4GHz Band Radio Type** drop-down lists, choose an interface rate.
- Valid backhaul interface rates are **802.11abg**, **802.11n**, **802.11ac** (5-GHz band radio only), **802.11ax**, and **Auto**, depending on the AP. Backhaul creates a wireless connection between the APs. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices.
- With the **Auto** data rate, each link can arrive at the best possible rate for its link quality.
- We recommend that you configure the mesh backhaul data rate as **Auto**.
- Step 7** (Optional) In the **Bridge Group Name** field in the **Bridge Group** area, enter a name of up to 10 characters for the bridge group.
- A bridge group name controls the association of MAPs. By grouping radios, two networks on the same channel, but in different bridge group names can't communicate with one another. This setting is also useful if you have more than one RAP in your network in the same sector (area).
- If you don't enter a bridge group name, Cisco DNA Center uses the **Default** bridge group name for the mesh profile.
-

What to do next

Configure the other necessary settings for the AP profile. For more information, see [Create an AP Profile for Cisco IOS XE Devices, on page 254](#).

Configure Power Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the following for an AP profile for Cisco IOS XE devices:

- **AP power profile:** If an AP doesn't receive the required power, it functions in a derated state based on the settings in the AP power profile. For more information, see [Create an AP Power Profile, on page 262](#).



Note The power settings are applicable only for the Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later.

- **Calendar power profile:** You can create calendar power profiles for APs that are in power save mode. You can map multiple AP power profiles to different calendar schedules as required. Based on the configured schedule, Cisco DNA Center runs all the rules defined in the AP power profiles simultaneously.

-
- Step 1** In the **Create Access Point Profile** window (**Design > Network Settings > Wireless > AP Profile** table > **Add > AP Profile for IOS-XE**), click the **Power** tab.
- Step 2** In the **AP Power Profile** area, from the **Select Value** drop-down list, choose a power profile.
(To create a power profile, click **Create New** and configure the parameters. For more information, see [Create an AP Power Profile, on page 262](#).)
- Step 3** In the **Calendar Power Profile** area, do the following:
- To add a calendar power profile, click **Add**. In the **Add Calendar Power Profile** slide-in pane, do the following:
 - From the **Select Power Profile** drop-down list, choose a power profile.
To create a power profile, click **Create New** and configure the parameters. For more information, see [Create an AP Power Profile, on page 262](#).
 - Choose the recurrence frequency for applying the power profile rules to the APs:
 - **Daily:** Applies the power profile rules to APs daily.
 - **Weekly:** Applies the power profile rules to APs every week on the selected days. Click the required day to select it.
 - **Monthly:** Applies the power profile rules to APs every month on the selected dates. Click the required date to select it.
 - Specify the start time and end time for the power profile rules.
 - Click **Save**.
 - (Optional) To edit a power profile rule, check the check box next to the corresponding power profile name and click **Edit**. In the **Edit Power Profile** slide-in pane, edit the required parameters and click **Save**.

- c) (Optional) To delete a power profile, check the check box next to the corresponding power profile name, click **Delete**, and then click **Yes**.

What to do next

Configure the other necessary settings for the AP profile. For more information, see [Create an AP Profile for Cisco IOS XE Devices, on page 254](#).

Configure Additional Settings for an AP Profile for Cisco IOS XE Devices

Use this procedure to configure the following for an AP profile for Cisco IOS XE devices:

- **Country code:** Set the country code for the Rest of World (ROW) domain APs that don't have a country code configured already.



Note The country code setting doesn't impact the APs that already have a country code configured.

- **Time zone:** Choose the time zone for the APs.
- **Client limit:** Specify the maximum number of allowed clients.

-
- Step 1** In the **Create Access Point Profile** window (**Design > Network Settings > Wireless > AP Profile table > Add > AP Profile for IOS-XE**), click the **Additional** tab.
- Step 2** In the **Country Code** area, from the **Select Value** drop-down list, choose a country for ROW APs that don't have a country code configured.
- Step 3** In the **Time Zone** area, choose one of the following options:
- **Not Configured:** APs operate in the UTC time zone.
 - **Controller:** APs operate in the Cisco Wireless Controller time zone.
 - **Delta from Controller:** APs operate in the offset time from the wireless controller time zone. Configure the following offset values:
 - **HH:** Enter the hour value. The valid range is from -12 through 14.
 - **MM:** Enter the minute value. The valid range is from 0 through 59.
- Step 4** In the **Client Limit** area, enter a value for the maximum client limit. The valid range is from 0 through 1200.
-

What to do next

After configuring all the necessary settings for the AP profile, click **Save**. For more information, see [Create an AP Profile for Cisco IOS XE Devices, on page 254](#).

Create an AP Profile for Cisco AireOS Devices

For Cisco AireOS devices, AP profiles group the AP-level parameters and configurations. AP profiles can be mapped to custom AP groups. When APs are provisioned, all the APs under the corresponding AP group are configured with the settings available in the AP profile.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** In the **AP Profile** table, hover your cursor over **Add** and choose **AP Profile for AireOS**.
- Step 5** In the **Create Access Point Profile** window, enter a name for the AP profile.
- Step 6** (Optional) Enter a description for the AP profile.
- Step 7** If this AP profile is for remote teleworker APs or Cisco OfficeExtend APs, check the **Remote Teleworker** check box.
- You can enable or disable the **Remote Teleworker** check box only while creating the AP profile. You can't update this option for existing AP profiles.
- Note** Remote teleworker-enabled AP profiles don't support the following settings:
- Rogue detection
 - Mesh
- Step 8** Configure the required settings in the followings tabs:
- a) **Management**: For more information, see [Configure Management Settings for an AP Profile for Cisco AireOS Devices, on page 260](#).
 - b) **Security**: For more information, see [Configure Security Settings for an AP Profile for Cisco AireOS Devices, on page 261](#).
 - c) **Mesh**: For more information, see [Configure Mesh Settings for an AP Profile for Cisco AireOS Devices, on page 261](#).
- Step 9** Click **Save**.
-

Configure Management Settings for an AP Profile for Cisco AireOS Devices

Use this procedure to configure the following for an AP profile for Cisco AireOS devices:

- Credentials for console access, SSH, and Telnet.
- Enable Cisco Discovery Protocol (CDP) to make the AP discoverable to its neighboring devices.

-
- Step 1** In the **Create Access Point Profile** window (**Design > Network Settings > Wireless > AP Profile** table > **Add > AP Profile for AireOS**), click the **Management** tab.
- Step 2** In the **SSH and Telnet** area, configure the following:
- a) (Optional) Click the **SSH** toggle button to configure the credentials for SSH.
 - b) (Optional) Click the **Telnet** toggle button to configure the credentials for Telnet.
 - c) In the **Username** field, enter the name used to authenticate the device.
- Username can't contain spaces or angle brackets (<>).

Note If you disable SSH and Telnet, the **Username** field is optional.

d) In the **Password** field, enter the password used to authenticate the device.

Note If you disable SSH and Telnet, the **Password** field is optional.

e) In the **Enable Password** field, enter the password to enable a higher privilege level in the CLI.

Note If you disable SSH and Telnet, the **Enable Password** field is optional.

Step 3 In the **Cisco Discovery Protocol (CDP) State** area, click the **CDP State** toggle button to enable or disable CDP.

What to do next

Configure the other necessary settings for the AP profile. For more information, see [Create an AP Profile for Cisco AireOS Devices, on page 260](#).

Configure Security Settings for an AP Profile for Cisco AireOS Devices

Use this procedure to configure rogue detection for an AP profile for Cisco AireOS devices. Rogue detection allows you to detect the APs that are installed on the network without explicit authorization from a system administrator.

Step 1 In the **Create Access Point Profile** window (**Design > Network Settings > Wireless > AP Profile table > Add > AP Profile for AireOS**), click the **Security** tab.

Step 2 In the **Rogue Detection** area, click the **Rogue Detection** toggle button to enable or disable rogue detection.

What to do next

Configure the other necessary settings for the AP profile. For more information, see [Create an AP Profile for Cisco AireOS Devices, on page 260](#).

Configure Mesh Settings for an AP Profile for Cisco AireOS Devices

Use this procedure to configure the mesh settings for an AP profile for Cisco AireOS devices.

Before you begin

Ensure that you add the MAC address of the MAP to the AP authorization list. For more information, see [Create an AP Authorization List, on page 250](#).

Step 1 In the **Create Access Point Profile** window (**Design > Network Settings > Wireless > AP Profile table > Add > AP Profile for AireOS**), click the **Mesh** tab.

Step 2 Click the **Mesh** toggle button.

Step 3 (Optional) In the **RAP Downlink Backhaul** area, click the radio button next to the required option.

If your country prohibits the use of **5 GHz**, choose **2.4 GHz**. Even if your country allows the use of **5 GHz**, consider using **2.4 GHz** because 2.4-GHz radio can cover larger mesh or bridge distances.

Note When you change the RAP configuration from **5 GHz** to **2.4 GHz**, Cisco DNA Center propagates the update from the RAP to all the MAPs. At this point, the MAPs disconnect from the 5-GHz network and connect to the 2.4-GHz network.

Step 4 (Optional) In the **Bridge Group Name** field in the **Bridge Group** area, enter a name of up to 10 characters for the bridge group.

A bridge group name controls the association of MAPs. By grouping radios, two networks on the same channel, but in different bridge group names, can't communicate with one another. This setting is also useful if you have more than one RAP in your network in the same sector (area).

If you don't enter a bridge group name, Cisco DNA Center uses the **Default** bridge group name for the mesh profile.

What to do next

After configuring all the necessary settings for the AP profile, click **Save**. For more information, see [Create an AP Profile for Cisco AireOS Devices, on page 260](#).

Edit or Delete an AP Profile

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **AP Profile** table, check the check box next to the AP profile that you want to edit or delete.

- To edit the AP profile, click **Edit**. In the **Edit Access Point Profile** slide-in pane, edit the configuration as necessary, and click **Save**. For more information, see [Create an AP Profile for Cisco AireOS Devices, on page 260](#) and [Create an AP Profile for Cisco IOS XE Devices, on page 254](#).
 - To delete the AP profile, click **Delete**, and then click **Yes**.
-

Create an AP Power Profile

You can create AP power profiles for Cisco Wireless Controllers running Cisco IOS XE Release 17.10.1 and later. Assign an AP power profile to APs by associating it to an AP profile. You can define multiple rules for an AP power profile and specify the sequences of rules.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.


Step 3 From the left hierarchy tree, choose **Global**.

Step 4 In the **AP Power Profile** table, click **Add**.

Step 5 In the **Create Power Profile** slide-in pane, enter a name for the AP power profile.

Step 6 (Optional) Enter a description for the AP power profile.


Step 7 To create a rule for the AP power profile, click **Add**.

- Step 8** In the **Rule** dialog box, configure the following:
- From the **Interface** drop-down list, choose a type of interface.
 - From the **Interface ID** drop-down list, choose an interface ID.
Note If only one interface ID is available, Cisco DNA Center automatically selects the available interface ID.
 - From the **Parameter** drop-down list, choose a parameter.
Note If only one parameter is available, Cisco DNA Center automatically selects the available parameter.
 - From the **Parameter Value** drop-down list, choose a parameter value.
Note If only one parameter value is available, Cisco DNA Center automatically selects the available parameter value.
 - Click **Add**.
- Step 9** (Optional) To create another rule for the AP power profile, repeat [Step 7, on page 262](#) and [Step 8, on page 263](#).
- Step 10** (Optional) To update the sequence of a rule in the **Rules** table, click the corresponding  icon, and drag and drop the rule to the required position.
- Step 11** Click **Save**.
-

What to do next

Associate the AP power profile with an AP profile. For more information, see [Create an AP Profile for Cisco IOS XE Devices, on page 254](#).

Edit or Delete an AP Power Profile

- Step 1** Click the menu icon () and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose **Global**.
- Step 4** In the **AP Power Profile** table, check the check box next to the AP power profile that you want to edit or delete.
- To edit the AP power profile, click **Edit**. In the **Edit Power Profile** slide-in pane, edit the description, rules, and sequence as necessary, and click **Save**. For more information, see [Create an AP Power Profile, on page 262](#).
 - To delete the AP power profile, click **Delete**, and then click **Yes**.
-

Provision a Cisco Sensor SSID for Nonfabric Deployment


- The Cisco DNA Center sensor uses the Cisco sensor provisioning Service Set Identifier (SSID) to communicate with the Plug and Play (PnP) server and obtain day-0 configurations for running tests.



Note The Cisco sensor provisioning SSID is not applicable for APs working as sensors.

- For fabric deployments, the Cisco sensor provisioning SSID is mapped to an Infrastructure Virtual Network Access Point (INFRA VN-AP) pool to communicate with Cisco DNA Center.
- The following platforms support the Cisco sensor provisioning SSID:
 - Cisco AireOS Controller
 - Cisco Catalyst 9800 Series Wireless Controller (both fabric and nonfabric deployments)
- The Cisco sensor provisioning SSID supports the following network controllers:
 - Cisco Catalyst 9800 Wireless Controllers for Cloud
 - Cisco Catalyst 9800 Series Wireless Controller
 - Cisco AireOS Controller

The following procedure enables you to configure the Cisco sensor provisioning SSID for nonfabric deployments.

- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the **SSID** table, hover over  and choose **Enterprise**.
The **Wireless SSID** workflow appears.
- Step 4** Toggle the **Sensor** field and click **Next**.
Note The parameters for the SSID are automatically populated and cannot be edited.
- Step 5** Click **Next**.
- Step 6** In the **Wireless Profiles** screen, check a profile from the **Profiles** table.
The **Edit Wireless Profile** dialog box appears.
- Step 7** In Fabric, select **Yes** and click **Save**.
The **Success Profile sensorProfile selected** message appears.
- Step 8** Click **Finish**.
- Step 9** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 10** Check a device and from the **Actions** drop-down menu, choose **Provision > Provision Device**.
- Step 11** Review the details under **Assign Site, Configuration, Model Configuration, Advanced Configuration, and Summary**.
Click **Next** after each screen.
- Step 12** Click **Deploy**.
The **Provision Device** dialog box is displayed.

Step 13 Choose **Now** and click **Apply**.

Result: The message **Task Scheduled view status in Tasks** appears at the bottom-right corner.

Manage Backhaul Settings

Use this procedure to view, create, and manage backhaul configurations for wireless sensors. A wireless sensor requires a backhaul SSID to communicate with Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Assurance > Manage > Sensors**.

The **Sensor List** window appears.

Step 2 Hover your cursor over the **Settings** tab and choose **Backhaul Settings**.

Step 3 You can add and manage backhaul SSIDs by doing the following:

a) Click **+ Add Backhaul**.

The **Create Sensor Backhaul SSID Assignment** window appears with two areas: **Wired Backhaul** and **Wireless Backhaul**.

b) In the **Settings Name** field, enter a name for the backhaul SSID.

c) In the **Wired Backhaul** area, configure the following:

- **Level of Security:** Displays the encryption and authentication type used by the selected SSID. The available security options are:

- **802.1x EAP:** Standard used for passing Extensible Authentication Protocol (EAP) over wired LAN.

- **Open:** No security or authentication is used.

- **EAP Method:** If you choose **802.1x EAP**, you must choose one of the following EAP methods for user authentication from the drop-down list:

- **EAP-FAST:** Enter the username and password in the fields provided.

- **PEAP-MSCHAPv2:** Enter the username and password in the fields provided.

- **EAP-TLS:** Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.

- **PEAP-TLS:** Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click **+ Add New Certificate Bundle**, and enter the username and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and configure the following.

- **Level of Security:** Displays the encryption and authentication type used by the selected SSID. The available security options are:

- **WPA2 Enterprise:** Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server.
- **WPA2-Personal:** Provides a good security using a passphrase or a preshared key (PSK). This allows anyone with the passkey to access the wireless network.

If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.

- **PSK Format:** The available preshared key formats are:
 - **ASCII:** Supports ASCII PSK passphrase.
 - **HEX:** Supports 64-character HEX key PSK password.
- **Open:** No security or authentication is used.

e) Click **Save**.

Step 4 You can edit the existing backhaul configurations by doing the following:

- Check the check box of the backhaul configuration.
- Hover your cursor over the **Actions** drop-down list and choose **Edit**.

Step 5 You can delete a backhaul configuration by doing the following:

- Check the check box of the backhaul configuration.
- Hover your cursor over the **Actions** drop-down list and choose **Delete**.

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of Cisco Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your wireless clients, rogue access points and interferers on the floor map within the Cisco DNA Center user interface.

Depending on your requirements, you can create CMX settings either at the global level or at the site, building, or floor level. For a small enterprise, you can assign CMX at the global level, which is the parent node. All children inherit their settings from the parent node. For a medium enterprise, you can assign CMX at the building level and for a small enterprise, you can assign CMX at the floor level.



Note CMX should be anonymized for security purposes.

Create Cisco CMX Settings

Step 1 Click the menu icon (☰) and choose **System > Settings**.

Step 2 From the **External Services** section, click **CMX Servers/Cisco Spaces**.

The **CMX Servers/Cisco Spaces** window opens.

Step 3 From the **CMX Servers** table, click **Add**.

- Step 4** Complete the fields in the **Add CMX Server** slide-in pane:
- **IP Address:** Enter the valid IP address of the CMX web GUI.
 - **User Name:** Enter the CMX web GUI username.
 - **Password:** Enter the password credentials.
 - **SSH User Name:** Enter the CMX admin username.
 - **SSH Password:** Enter the CMX admin password credentials.

Note Make sure that CMX is reachable.

- Step 5** Click **Add**.
The CMX server is added successfully.

Step 6 To assign a CMX server to a site, building, or a floor, click the menu icon and choose **Design > Network Settings**.

Step 7 Click the **Wireless** tab.

Step 8 From the left hierarchy tree, choose either **Global** or the required area, building, or floor.

Step 9 In the **CMX Servers/Cisco Spaces** section, use the drop-down list, choose the CMX server.

Step 10 Click **Save**.

The **Create CMX Settings** window opens.

After the CMX is added, if you make any changes to the floor on the **Network Hierarchy** page, the changes are synchronized automatically with the CMX.

When the CMX is synced, Cisco DNA Center starts querying the CMX for the client location and displays the location on the floor map.

Step 11 From the floor map, you can do the following:

- View the location of the client, which is shown as a blue dot.
- Hover your cursor over an AP. A dialog box is displayed with **Info**, **Rx Neighbor**, and **Clients** tabs. Click each tab for more information. Click **Device 360** to open the Device 360 window and view issues. Click an issue to see the location of the issue and the location of the client device.
- Click an AP to open a side bar with details about the AP.
- Perform real-time client tracking when Intelligent Capture and CMX are integrated.

Step 12 If the CMX was down when you made changes, you must synchronize manually. To do so, on the **Network Hierarchy** page, hover your cursor over the ellipsis **...** next to the building or floor on which you made the changes in the left hierarchy tree, and then choose **Sync: CMX Server/Cisco Spaces** to push the changes manually.

Step 13 To edit the CMX server details or delete a CMX server, do the following:

- a) Click the menu icon (**☰**) and choose **System > Settings**.
- b) From the **External Services** section, click **CMX Servers/Cisco Spaces**.
- c) Select the CMX server that you want to edit, make any changes, and click **Update**.
- d) Select the CMX server that you want to delete and click **Delete**.
- e) Click **OK** to confirm the deletion.

For CMX Authentication Failure

- Check if you are able to log in to the CMX web GUI with the credentials that you provided at the time of CMX settings creation on Cisco DNA Center.
- Check if you are able to log in to the CMX console using SSH.
- Check if you are able to exercise CMX REST APIs using the API Documentation link on the CMX GUI.

If Clients Do Not Appear on the Cisco DNA Center Floor Map

- Check if the Cisco wireless controller on the particular floor is configured with CMX and is active.
- Check if the CMX GUI shows clients on the floor map.
- Use the Cisco DNA Center Maps API to list the clients on the floor:

```
curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true
```

About Cisco Spaces Integration

Enterprises operating in the physical world have limited to no visibility into the behavior of people and connected assets within their buildings. Cisco Spaces solves this physical blind-spot problem using location-sensing intelligence from all underlying Cisco wireless networks and translating the data into business-ready insights.

Cisco DNA Center integrates with Cisco Spaces to provide you with the exact location of wireless clients, rogue APs, and interferers on Cisco DNA Center floor maps. Depending on your requirements, you can create Cisco Spaces settings either at the global level or at the site, building, or floor level.

When you assign Cisco Spaces at the global level or at the site, building, or floor level, Cisco DNA Center automatically sends the floor map configuration to Cisco Spaces. Similarly, any time you save a change to a floor map, Cisco DNA Center automatically synchronizes the floor map configuration with Cisco Spaces. Synchronization occurs serially; one floor map doesn't start to synchronize until the previously configured floor map synchronization is completed. So, if multiple floors are configured in close succession, it can take a long time to complete.

You can also trigger a manual synchronization of floor maps to Cisco Spaces. However, we recommend that you use discretion when using this option. When a manual synchronization is triggered, the Cisco DNA Center GUI hangs until the synchronization has completed and Cisco DNA Center returns a response to indicate the synchronization success or failure. Additionally, if an automatic synchronization is already in progress when a manual synchronization is triggered, the manual synchronization won't start until the automatic synchronization is done. While waiting for the automatic synchronization to end and during the manual synchronization itself, the Cisco DNA Center GUI hangs. In these cases, depending on the number of floor maps contained in the site, the Cisco DNA Center GUI could hang for a long period.

Therefore, you should use the manual synchronization option only in the unlikely event that the automatic map synchronization to Cisco Spaces fails due to a network issue or a temporary service outage. The manual synchronization option should not be used on a consistent basis to update floor map changes with to Cisco Spaces.

To integrate Cisco Spaces with Cisco DNA Center, see the "Cisco DNA Center Integration" section in the [Cisco Spaces Configuration Guide](#).

Assign Cisco Spaces to Sites

To monitor sites using Cisco Spaces, you need to assign Cisco Spaces to the site that you want to monitor.

Before you begin

Integrate Cisco Spaces with Cisco DNA Center. For details, see the [Cisco Spaces Configuration Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings**.
- Step 2** Click the **Wireless** tab.
- Step 3** From the left hierarchy tree, choose either **Global** or the area, building, or floor to which you want to assign Cisco Spaces.
- Step 4** Click **DNA Spaces/CMX Servers**.
- Step 5** In the **DNA Spaces/CMX Servers** section, from the **Location Services** drop-down list, select a site.
- Step 6** Click **Save**.
- Cisco DNA Center deploys the site information to Cisco Spaces automatically.
-

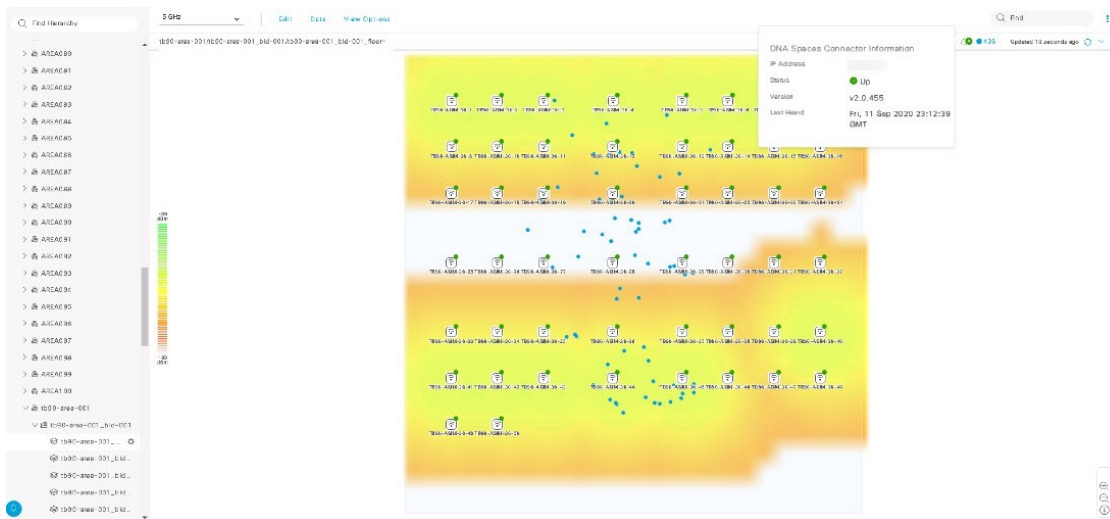
Monitor Sites Using Cisco Spaces

You can monitor sites using Cisco Spaces.

Before you begin

- Integrate Cisco Spaces with Cisco DNA Center. For details, see the [Cisco Spaces Configuration Guide](#).
- Assign Cisco Spaces to the site that you want to monitor.

-
- Step 1** In the Cisco DNA Center GUI, click the menu icon (☰) and choose **Design > Network Hierarchy**.
- Step 2** From the left hierarchy tree, choose either **Global** or the area, building, or floor that you want Cisco Spaces to monitor.
- Step 3** To confirm that Cisco Spaces is operational, verify that the Cisco Spaces/CMX status icon displays on the floor that you want to monitor, as shown in the following figure.



Configure a FlexConnect VLAN

You can configure the following FlexConnect VLAN settings:

- **Native VLAN:** Allows a FlexConnect group to carry the management traffic between APs and Cisco Wireless Controllers.
- **AAA Override VLAN:** Provides dynamic VLAN assignment of locally switched clients.

You can apply these settings at the global level and override them at the site, building, or floor level.

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 Click the **Wireless** tab.

Step 3 From the left hierarchy tree, choose the required site:

- **Global:** Configures the VLAN at the global level for all sites.
- **Area, building, or floor:** Configures the VLAN at the chosen level only.

Step 4 In the **Native VLAN ID** field, enter a value for the VLAN ID. The valid range is from 1 through 4094.

Step 5 For the **AAA Override VLAN** settings, enter a VLAN ID and VLAN name mapping in the corresponding **VLAN ID** and **VLAN Name** fields. To add more mappings, click the Add icon.

Note The maximum number of VLAN mappings that you can define for a FlexConnect deployment is 16. However, for Cisco Catalyst 9800 Series Wireless Controllers, this number includes default WLAN VLANs and VLANs pushed by AAA.

Step 6 Click **Save**.

What to do next

Create a wireless network profile *or* configure an SSID:

- **Wireless Network Profile:** If you decide to create a wireless network profile, make sure that the **FlexConnect Local Switching** check box is checked. For more information, see [Create Network Profiles for Wireless, on page 281](#).
- **SSID:** If you want to configure an SSID, see [Create SSIDs for an Enterprise Wireless Network, on page 207](#) and [Create SSIDs for a Guest Wireless Network, on page 216](#).

For the saved FlexConnect VLAN settings to get configured on the wireless controller, you must provision the wireless controller. For information, see [Provision a Cisco AireOS Controller, on page 391](#) or [Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 403](#).

After provisioning the wireless controller, you must provision the AP that is associated with the controller.

About Wireless Mesh Networks

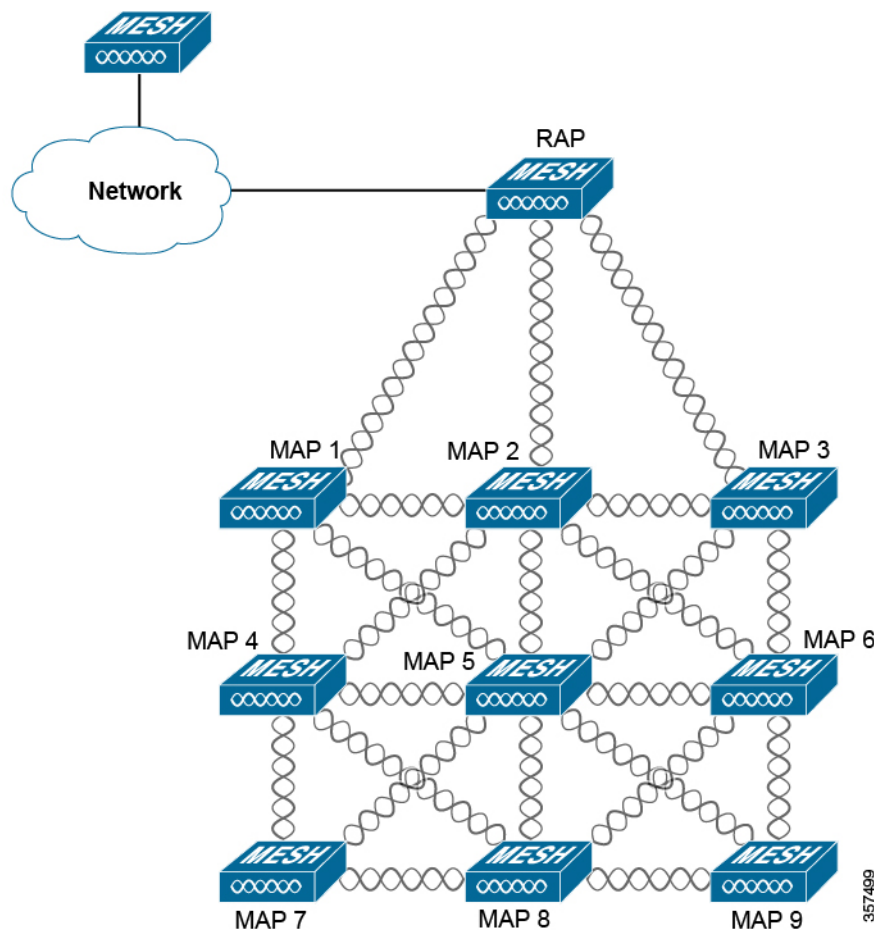
In a Cisco wireless mesh network, Access Points (APs) operate in one of the following two ways:

- Root Access Point (RAP): Connected to the wired network at each location.
- Mesh Access Point (MAP): Communicate wirelessly while providing secure and scalable wireless LAN.



Note All APs are configured and shipped as MAPs. To use an AP as a RAP, you must reconfigure it as a RAP. In all mesh networks, make sure that there is at least one RAP.

RAPs are connected to the wired network at each location. All the downstream APs operate as MAPs and communicate using wireless links.



Both MAPs and RAPs can provide WLAN client access. However, typically, the location of RAPs is often not suitable for providing client access.

Some buildings have onsite controllers to terminate CAPWAP sessions from the MAPs, but it's not a mandatory requirement because CAPWAP sessions can be backhauled to a controller over a wide-area network (WAN).

In a Cisco wireless backhaul network, traffic can be bridged between MAPs and RAPs. This traffic can be from wired devices that are being bridged by the wireless mesh or CAPWAP traffic from the MAPs. This traffic is always AES encrypted when it crosses a wireless mesh link such as a wireless backhaul.

For more information about mesh networks, see the latest [Cisco Wireless Mesh Access Points, Design and Deployment Guide](#).

Cisco Wireless Controller Configuration

For mesh networks, you need to configure a list of authorized APs in the controllers. Controllers respond only to requests from the MAPs that are present in its authorization list.



Note Cisco DNA Center supports the configuration of authorization lists on Cisco Catalyst 9800 Series Wireless Controller running Cisco IOS Release 17.5 and later.

Both Cisco AireOS Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller can use Cisco DNA Center to configure the Bridge Group Name (BGN) and RAP downlink backhaul mesh settings. In Cisco Catalyst 9800 Series Wireless Controller, you can also configure the maximum range of the MAPs, backhaul client access, and backhaul data rates.

These settings are configured for the global site in the **Create AP Profile** window. For more information, see [Configure Mesh Settings for an AP Profile for Cisco IOS XE Devices, on page 256](#) and [Configure Mesh Settings for an AP Profile for Cisco AireOS Devices, on page 261](#).

AP Configuration

If you have existing APs that you want to use in mesh network mode, you must first change the AP Mode to Bridge or Flex+Bridge using the **Configure Access Point** workflow. For information, see [Configure AP Workflow, on page 716](#).

After an AP is configured for Bridge or Flex+Bridge mode, the **AP 360** window shows the mesh configuration. At this point, you need to provision the APs with the new configuration. [Provision a Cisco AP—Day 1 AP Provisioning, on page 397](#).

Configure a Certificate Revocation Check

Use the following steps to configure a certificate revocation check.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Security and Trust**.
 - Step 2** From the left hierarchy tree, choose a site, building, or floor.
 - Step 3** In the **Revocation Check** drop-down list, **Revocation - Check: CRL None** is selected by default.
 - Step 4** To skip the revocation check, choose **Revocation - Check: None** and click **Save**.
-



CHAPTER 10

Configure Network Profiles

- [Network Profiles Overview, on page 275](#)
- [Create Network Profiles for Assurance, on page 275](#)
- [Create Network Profiles for Firewall, on page 277](#)
- [Create Network Profiles for Routing, on page 278](#)
- [Create Network Profiles for Switching, on page 280](#)
- [Create Network Profile for Cisco DNA Traffic Telemetry Appliance, on page 281](#)
- [Create Network Profiles for Wireless, on page 281](#)

Network Profiles Overview

Network profiles allow you to configure settings and apply them to a specific site or group of sites. You can create network profiles for various elements in Cisco DNA Center:

- [Create Network Profiles for Assurance, on page 275](#)
- [Create Network Profiles for Firewall, on page 277](#)
- [Create Network Profiles for Routing, on page 278](#)
- [Create Network Profiles for Switching, on page 280](#)
- [Create Network Profile for Cisco DNA Traffic Telemetry Appliance, on page 281](#)
- [Create Network Profiles for Wireless, on page 281](#)

Create Network Profiles for Assurance

Creating a network profile for Assurance allows you to configure issue settings and apply them to a site or group of sites independently from the global issues settings. You can enable or disable an issue, and you can change its priority.

Notes:

- In Assurance, synchronization to the network device health score is available only for global issue settings, not custom issue settings. For information, see the [Cisco DNA Assurance User Guide](#).

- Some global issues are not customizable. These issues are not displayed in the list of custom issues for you to modify.
- To display modified issues at the top of the list, sort by **Last Modified**.
- To delete custom settings, you must first unassign all the sites.

Step 1 Click the menu icon (☰) and choose **Design > Network Profiles**.

Step 2 Click **+Add Profile** and choose **Assurance**.

Step 3 In the **Profile Name** field, enter a valid profile name and click **Next**.

Cisco DNA Center adds the profile and the **Edit Profile** window appears.

Step 4 Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues you want to configure.

Step 5 Click an issue in the **Issue Name** column to open a slide-in pane with the settings.

Note For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, Cisco DNA Center displays a caution that indicates the affected device types.

Step 6 To enable or disable whether Cisco DNA Center monitors the issue, click the **Enabled** toggle button.

Step 7 To set the issue priority, click the **Priority** drop-down list and select the priority. The options are:

- **P1**: A critical issue that needs immediate attention and can have a wide impact on network operations.
- **P2**: A major issue that can potentially impact multiple devices or clients.
- **P3**: A minor issue that has a localized or minimal impact.
- **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

Step 8 (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Examples of a trigger condition:

`No Activity on Radio(2.4 GHz) >= 60 minutes.`

`Memory Utilization of Access Points greater than 90%.`

Step 9 (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default settings. Click **Use Default** to restore all the issue settings to the default values.

Step 10 Click **Apply**.

Step 11 (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered.

Step 12 To assign the profile to sites, click **Assign Sites**. Check the check box next to the sites that you want to associate with this profile and click **Save**.

The **Edit Profile** window appears.

Note You can select a parent node or the individual sites. If you select a parent node, all the children under the parent node are also selected. You can uncheck the check box to deselect a site.

Step 13 Click **Done**.

The newly added profile appears on the **Network Profiles** window.

Create Network Profiles for Firewall

This workflow shows how to:

1. Create custom configurations.
2. Create Firepower Threat Defense (FTD) configurations.
3. View the profile summary.

Step 1 Click the menu icon (☰) and choose **Design > Network Profiles**.

Step 2 Click **+Add Profile** and choose **Firewall**.

The **Firewall Type** page appears.

Step 3 To create custom configurations for regular firewalls like Adaptive Security Appliance (ASA) firewalls, do the following:

- a) In the **Name** field, enter the profile name.
- b) Choose the number of devices from the **Devices** drop-down list.

Note You can choose up to 10 devices per profile.

- c) Choose the type of device from the **Device Type** drop-down list.
- d) (Optional) From the **Device Tag** drop-down list, choose the device tags.
- e) Click **Next**.

The **Custom Configuration** page appears.

- f) From the **Template** drop-down list, choose a template.

Note If there are no templates, you must create at least one template in **Tools > Template Hub**. For information, see [Create Templates, on page 293](#).

- g) Click **Next**.

The **Summary** page appears. This page summarizes the custom configurations. Based on the selected device type, a hardware recommendation is provided.

- h) Click **Save**.

The **Network Profiles** page appears.

- i) To assign a site to the network profile, click **Assign Sites**. For more information, see [Create, Edit and Delete a Site, on page 134](#).

Step 4 To create FTD configurations to configure the FTD devices, do the following:

- a) In the **Name** field, enter the profile name.
- b) From the **Devices** drop-down list, choose the number of devices.

Note You can choose up to 10 devices per profile.

- c) To provision an FTD firewall, check the **FTD** check box.
- d) From the **Device Type** drop-down list, choose the type of device.
- e) (Optional) Choose the device tags from the **Device Tag** drop-down list.
- f) Click **Next**.

The **FTD Configuration** page appears.

- g) Click the **Routed Mode** or **Transparent Mode** radio button.
- h) Click **Next**.

The **Summary** page appears. This page summarizes the FTD configurations. Based on the selected device type, hardware recommendation is provided on this page.

- i) Click **Save**.


The **Network Profiles** page appears.

- j) To assign a site to the network profile, click **Assign Sites**. For information, see [Create, Edit and Delete a Site, on page 134](#).

Create Network Profiles for Routing

This workflow shows how to:

1. Configure the router WAN.
2. Configure the router LAN.
3. Configure the integrated switch configuration.
4. Create custom configurations.
5. View the profile summary.

Step 1 Click the menu icon () and choose **Design > Network Profiles**.

Step 2 Click **+Add Profile** and choose **Routing**.

Step 3 The **Router WAN Configuration** window appears.

- Enter the profile name in the **Name** text box.
- Select the number of **Service Providers** and **Devices** from the drop-down list. Up to three service providers and ten devices are supported per profile.
- Select the **Service Provider Profile** from the drop-down list. For more information, see [Configure Service Provider Profiles, on page 207](#).
- Select the **Device Type** from the drop-down list.
- Enter a unique string in the **Device Tag** to identify the different devices, or select an existing tag from the drop-down list. Use the device tag if two or more devices are of the same type. If all the devices are of a different type, the device tag is optional. Select the appropriate tag, because your selection is used as part of the matching criteria for Day-0 and Day-N templates applied to the network profile.

- To enable at least one line link for each device to proceed, click **O** and check the check box next to **Connect**. Select the **Line Type** from the drop-down list. Click **OK**.

If you select multiple service providers, you can select the primary interface as gigabit Ethernet and the secondary as cellular, or both the interfaces as gigabit Ethernet. You can also select the primary interface as cellular and the secondary interface as gigabit Ethernet.

Note Only Cisco 1100 Series Integrated Services Routers, Cisco 4200 Series Integrated Services Routers, Cisco 4300 Series Integrated Services Routers, and Cisco 4400 Series Integrated Services Routers support the cellular interface.

- Click **Next**.

Step 4 The **Router LAN Configuration** page appears.

- Click the **Configure Connection** radio button and choose L2, L3, or both.
- If you choose **L2**, select the **Type** from the drop-down list and enter the **VLAN ID/Allowed VLAN** and the **Description**.
- If you choose **L3**, select the **Protocol Routing** from the drop-down list and enter the **Protocol Qualifier**.

You can click **Skip** to skip the configuration.

- Click **Next**.

Step 5 The **Integrated Switch Configuration** page appears.

The integrated switch configuration allows you to add new VLANs or retain the previous configuration selected in the router LAN configuration.

- To add one or more new VLANs, click **+**.
- To delete a VLAN, click **x**.
- Click **Next**.

Note Switchport Interface support is available only for Cisco 1100 Series and Cisco 4000 series Integrated Services Routers.

Step 6 The **Custom Configuration** page appears.

The custom configurations are optional. You can skip this step and apply the configurations at any time in the Network Profiles page.

If you choose to add custom configurations:

- Click the **Onboarding Template(s)** or **Day-N Templates** tab, as required.
- Choose a template from the drop-down list. The templates are filtered by **Device Type** and **Tag Name**.
- Click **Next**.

Step 7 On the **Summary** page, click **Save**.

This page summarizes the router configurations. Based on the devices and services selected, the hardware recommendation is provided.

Step 8 The **Network Profiles** page appears.

Click **Assign Sites** to assign a site to the network profile. For more information, see [Create, Edit and Delete a Site, on page 134](#).

Create Network Profiles for Switching

You can apply two types of configuration templates to a switching profile:

- Onboarding template
- Day N template

Before you begin

Define the **Onboarding Configuration** template that you want to apply to the devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. See [Create Templates to Automate Device Configuration Changes, on page 291](#).

Step 1 Click the menu icon (☰) and choose **Design > Network Profiles**.

Step 2 Click **+Add Profile** and choose **Switching**.

Step 3 In the Switching profile window, enter the profile name in the **Profile Name** text box.

Depending on the type of template that you want to create, click **OnBoarding Template(s)** or **Day-N Template(s)**.

- Click **+Add**.
- Select **Switches and Hubs** from the **Device Type** drop-down list.
- Select the **Tag Name** from the drop-down list. This step is optional. If the tag that you selected has already been associated with a template, only that template is available in the Template drop-down list.
- Select the **Device Type** from the drop-down list.
- Select a **Template** from the drop-down list. You can select the Onboarding Configuration template that you have already created.

Step 4 Click **Save**.

The profile that is configured on the switch is applied when the switch is provisioned. Note that you must add the network profile to a site for it to be effective.

Create Network Profile for Cisco DNA Traffic Telemetry Appliance

Before you begin

Define the template that you want to apply to the telemetry appliances. See [Create Templates to Automate Device Configuration Changes, on page 291](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Profiles**.
- Step 2** Click **+Add Profile** and choose **Telemetry Appliance**.
- Step 3** In the **Telemetry Appliance Type** window, complete the following:
- Enter the profile name in the **Name** text box.
 - From the **Devices** drop-down list, choose the number of devices.
 - From the **Device Tag** drop-down list, choose an existing device tag defined in Cisco DNA Center or enter a new tag. This step is optional. If the tag that you selected has already been associated with a template, only that template is available in the Template drop-down list.
 - Click **Next**.
- Step 4** In the **Custom Configuration** window, choose the template. The chosen template will be applied to the device once it is managed in Cisco DNA Center inventory.
- Step 5** Click **Next**.
- Step 6** In the **Summary** window, click **Save**.
-

Create Network Profiles for Wireless

Before you begin

- Ensure that you have created wireless SSIDs, RF profiles, and AP profiles under the **Design > Network Settings > Wireless** tab.
 - If necessary, ensure that you have created templates in the **Tools > Template Hub** window.
 - If necessary, ensure that you have created model configuration designs in the **Tools > Model Config Editor** window.
-

- Step 1** Click the menu icon (☰) and choose **Design > Network Profiles**.
- Step 2** Click **Add Profile** and choose **Wireless**.
- Step 3** Enter a valid profile name in the **Profile Name** field.
- Step 4** To add sites to the profile, click **Assign** and do the following:
- In the **Add Sites to Profile** slide-in pane, check the check box next to the sites that you want to associate with this profile.

You can select a parent node or the individual site. If you select a parent site, all the children under the parent node are also selected. Note that you can uncheck the check box to deselect a site.

b) Click **Save**.

Step 5 Configure the required settings in the following tabs:

- **SSIDs:** For more information, see [Add SSIDs to a Network Profile, on page 282](#).
- (Optional) **AP Zones:** For more information, see [Add AP Zones to a Network Profile, on page 283](#).
- **Model Configs:** For more information, see [Add Model Configurations to a Network Profile, on page 284](#).
- **Templates:** For more information, see [Add Templates to a Network Profile, on page 285](#).
- (Optional) **Advanced Settings:** For more information, see [Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 285](#).

Step 6 Click **Save** to add the network profile.

Cisco DNA Center displays the new network profile on the **Design > Network Profiles** window.

Add SSIDs to a Network Profile

Before you begin

Ensure that you have created wireless SSIDs under the **Design > Network Settings > Wireless** tab.

Step 1 In the **Add a Network Profile** window (**Design > Network Profiles > Add Profile > Wireless**), click the **SSID** tab.

Step 2 Click **Add SSID**.

Step 3 From the **SSID** drop-down list, choose the SSID that you have already created.

Step 4 (Optional) In the **WLAN Profile Name** field, enter a name for the WLAN profile.

Based on the WLAN profile name, Cisco DNA Center automatically generates the policy profile name.

Note When an SSID is associated with a network profile, Cisco DNA Center uses this WLAN profile name during provisioning. If you need to associate an SSID with multiple network profiles, ensure that the WLAN profile name is unique for the SSID across all network profiles to prevent provisioning failure.

Step 5 Specify whether the SSID is fabric or nonfabric using the **Yes** or **No** radio buttons.

To create a nonfabric SSID, click **No**, and configure the following parameters:

- Click the **Enable SSID Scheduler** toggle button and choose the scheduler from the drop-down list.
- To use an interface for traffic switching, click the **Interface** radio button. From the **Interface Name** drop-down list, choose an interface name for the SSID, or click the plus icon (+) to create a wireless interface.
- To use a VLAN group for traffic switching, click the **VLAN Group** radio button. From the **VLAN Group Name** drop-down list, choose a VLAN group name for the SSID, or click the plus icon (+) to create a VLAN group.

- In the **Do you need Anchor for this SSID?** area, click **Yes** to add an anchor to the SSID. By default, **No** is selected.
- If you choose **Yes**, from the **Select Anchor Group** drop-down list, choose an anchor group for the SSID. For more information about anchor groups, see [Create an Anchor Group, on page 252](#).
- If you choose **No**, check the **Flex Connect Local Switching** check box to enable local switching for WLAN.


If you choose to add an anchor to the SSID, you can't enable **Flex Connect Local Switching**.

If you enable **Flex Connect Local Switching** for an SSID, all the APs on the floor where the network profile is mapped, switch to FlexConnect mode.

The **Flex Group** option is enabled in the **Advanced Settings** tab. For more information, see [Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 285](#).

When you enable local switching, any FlexConnect AP that advertises this WLAN can locally switch data packets.

- If you have enabled the **Flex Connect Local Switching** check box, enter a value for the VLAN ID in the **Local to VLAN** field.

Step 6 (Optional) To add another SSID, click the plus icon () and configure its parameters.

What to do next

Configure the other necessary settings for the network profile. For more information, see [Create Network Profiles for Wireless, on page 281](#).

Add AP Zones to a Network Profile

An AP zone allows you to associate different SSIDs and RF profiles for a set of APs on the same site. You can use device tags to identify the APs for which you want to apply AP zone. From the **AP Zones** tab, you can create separate AP zones with a subset of SSIDs configured in the network profile for a device tag.

Cisco DNA Center applies the AP zone configurations to APs during AP provisioning.




- Note**
- Cisco DNA Center doesn't apply AP zone configurations to the APs claimed from the Plug and Play (PnP) process.
 - If you update the AP zone configuration, you must reprovision the wireless controller. After reprovisioning the wireless controller, you must provision the AP to apply the AP zone configuration changes to the AP.

During AP provisioning:

- Based on the device tag and site of the AP, Cisco DNA Center selects the corresponding AP zone and automatically assigns the RF profile.
- If two AP zones are configured for an AP, you can choose the required AP zone.
- If there are no AP zones for an AP, you can choose the required RF profile.

Before you begin

Ensure that you have created wireless SSIDs under the **Design > Network Settings > Wireless** tab.

-
- Step 1** In the **Add a Network Profile** window (**Design > Network Profiles > Add Profile > Wireless**), click the **AP Zones** tab.
- Step 2** Click **Add AP Zone**.
- Step 3** In the **AP Zone Name** field, enter a name for the AP zone.
- Step 4** From the **Device Tags** drop-down list, check the check box next to the device tags that you want to choose.
- Step 5** From the **RF Profile** drop-down list, choose an RF profile.
- Step 6** From the **SSID** drop-down list, choose the SSIDs.
- Step 7** (Optional) To add another AP zone, click the plus icon () and configure its parameters.
-

What to do next

Configure the other necessary settings for the network profile. For more information, see [Create Network Profiles for Wireless, on page 281](#).

To apply the AP zone configuration to an AP:

1. Reconfigure the wireless controller. For more information, see [Provision a Cisco AireOS Controller, on page 391](#) and [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).
2. Provision the AP. For more information, see [Provision a Cisco AP—Day 1 AP Provisioning, on page 397](#).

Add Model Configurations to a Network Profile

You can attach model configuration designs to a network profile.

-
- Step 1** In the **Add a Network Profile** window (**Design > Network Profiles > Add Profile > Wireless**), click the **Model Configs** tab.
- Step 2** Click **Add Model Config**.
- Step 3** In the **Add Model Config** slide-in pane, do the following:
- a. Click **Device Type(s)** and choose a device type.
You can either search for a device name by entering its name in the **Search** field, or expand **Switches and Hubs** or **Wireless Controller** and choose a device type.
 - b. Expand **Wireless** and choose the model configuration designs that you want to attach to this network profile.
 - c. From the **Tags** drop-down list under **APPLICABILITY**, choose the applicable tags.
 - d. Click **Add**.
-

What to do next

Configure the other necessary settings for the network profile. For more information, see [Create Network Profiles for Wireless, on page 281](#).

Add Templates to a Network Profile

You can associate a template with a network profile.

Step 1 In the **Add a Network Profile** window (**Design > Network Profiles > Add Profile > Wireless**), click the **Templates** tab.

Step 2 Click the plus icon (+).

Step 3 In the **Add Template** slide-in pane, do the following:

- a. From the **Device Type(s)** drop-down list, choose a device type.

You can either search for a device name by entering its name in the **Search** field, or expand **Wireless Controller** and choose a device type.

- b. In the **Template** area, choose a template.

- c. From the **Select Value** drop-down list under **APPLICABLE DEVICE TAGS**, choose the device tags.

You can use tags on templates only when you have to push different templates for the same device type based on the device tag.

- d. Click **Add**.

What to do next

Configure the other necessary settings for the network profile. For more information, see [Create Network Profiles for Wireless, on page 281](#).

Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile

Cisco DNA Center allows you to add AP groups, flex groups, site tags, and policy tags in a network profile. Preprovisioning AP groups and flex groups saves time during AP provisioning by eliminating the need to make repetitive configuration changes and ensures consistency across your devices. You can define custom names for AP groups, site tags, and policy tags in the **Advanced Settings** tab.



Note Flex group configuration is available only when the network profile has at least one associated flex-based SSID.

Cisco DNA Center configures and applies the newly added custom names specified in the **Advanced Settings** tab to the APs during Cisco Wireless Controller provisioning. If you don't configure the custom names, Cisco DNA Center uses the autogenerated AP group names and tags for the APs.

**Note**

- AP group and flex group configuration are applicable to the Cisco AireOS Wireless Controller.
- Site tag and policy tag configuration are applicable to the Cisco Catalyst 9800 Series Wireless Controller.

Newly added site tag and policy tag configurations are applied when you provision the APs. Provisioning the wireless controller alone won't configure the new custom tags on the APs. You must reconfigure the wireless controller or the APs if there are any modifications to the tags after provisioning.

Note the following scenarios while provisioning or reconfiguring the wireless controller and APs:

- If there are no custom site or policy tags configured on the network profile, then Cisco DNA Center uses the auto-generated tags and configures it on the wireless controller and applies to the APs only during AP provisioning.
- If there are custom site or policy tags configured on the network profile, then Cisco DNA Center configures the custom tags on the wireless controller and applies to the APs only during AP provisioning.
- If the wireless controller and AP are already provisioned with auto-generated tags and if you create new custom tags in the network profile, then you must reconfigure the wireless controller or the AP to apply the changes.

- If the wireless controller and AP are already provisioned with custom tags and if you delete the custom tags from the network profile, then you must reconfigure the wireless controller or the APs.

Reconfiguring the wireless controller deletes the custom tag configurations and configures the auto-generated tags on the wireless controller and the associated APs.

Reconfiguring the APs directly, without reconfiguring the wireless controller, configures the auto-generated tags on the APs but does not delete the custom tag configurations from the wireless controller. The tags are deleted during the next wireless controller reconfiguring.

- If you've upgraded to Cisco DNA Center with FlexConnect Native VLAN override configured and site tags that are mapped to the same custom Flex profile for all the floors in a site, then you must reconfigure the network profile with different site tags for each floor or else provisioning may fail.

You can use the same AP group and flex group across sites (buildings or floors) within an area. However, you can't reuse the same AP group and flex groups across multiple areas in the network hierarchy. Child sites inherit the AP group and flex groups from their parent sites. However, if you create AP group or flex group for a child site, it overrides the settings inherited from its parent site. If an SSID is overridden for different floors in a building, you can't reuse the AP groups or flex groups for such floors.

Before you begin

- Ensure that you have assigned a site to the network profile.
- To create flex group names, under the **SSIDs** tab, ensure that you have checked the **Flex Connect Local Switching** check box and defined the VLAN ID in the **Local to VLAN** field to mark the nonfabric SSID as a flex-based SSID. For more information, see [Add SSIDs to a Network Profile, on page 282](#).

If you have enabled **Flex Connect Local Switching** for an SSID, all the APs on the floor where the network profile is mapped, switch to FlexConnect mode.

- Step 1** In the **Add a Network Profile** window, click the **Advanced Settings** tab.
- Step 2** To create an AP group in the network profile, expand **AP Groups and AP Profiles** and click **Create Custom AP Group**.
In the **Add AP Group** window, do the following:
- In the **AP Group Name** field, enter the AP group name.
 - From the **AP Zone** drop-down list, choose an AP zone.
To broadcast all the SSIDs associated with the network profile, choose **Not Applicable**.
- Note** This drop-down list is enabled if you have added AP zones to the network profile in the **AP Zones** tab. For more information, see [Add AP Zones to a Network Profile, on page 283](#).
- If you choose an AP zone, the RF profile is inherited from the AP zone configuration.
- From the **AP Profile** drop-down list, choose an AP profile.
To create an AP profile, click **Create New**. For more information, see [AP Profiles, on page 253](#).
 - From the **RF Profile** drop-down list, choose an RF profile.
- Note** This drop-down list is disabled if you choose an AP zone from the **AP Zone** drop-down list.
- In the **Select Sites** area, you can either search for a site by entering its name, or expand **Global** to choose a site.
 - Click **Save**.
- Step 3** To create a flex group in the network profile, expand **Flex Group** and click **Create Flex Group**.
In the **Create Flex Group** window, do the following:
- In the **Flex Group Name** field, enter the flex group name.
 - In the **Select Sites** area, you can either search for a site by entering its name, or expand **Global** to choose a site.
 - Click **Save**.
- Step 4** To create a site tag in the network profile, expand **Site Tags and AP Profiles** and click **Create Custom Site Tag**.
In the **Create Site Tag** window, do the following:
- In the **Site Tag Name** field, enter the site tag name.
 - From the **AP Profile** drop-down list, choose an AP profile.
To create an AP profile, click **Create New**. For more information, see [AP Profiles, on page 253](#).
 - In the **Flex Profile Name** field, enter the flex profile name.
- Note** To enable the **Flex Profile Name** field, check the **Flex Connect Local Switching** check box in the **SSID** tab. For more information, see [Add SSIDs to a Network Profile, on page 282](#).
- In the **Select Sites** area, you can either search for a site by entering its name, or expand **Global** to choose a site.
 - Click **Save**.
- Step 5** To create a policy tag in the network profile, expand **Policy Tag** and click **Create Policy Tag**.
In the **Create Policy Tag** window, do the following:
- In the **Policy Tag Name** field, enter the policy tag name.
 - From the **AP Zone** drop-down list, choose an AP zone.

Note This drop-down list is enabled if you have added AP zones to the network profile in the **AP Zones** tab. For more information, see [Add AP Zones to a Network Profile, on page 283](#).

- c) In the **Select Sites** area, you can either search for a site by entering its name, or expand **Global** to choose a site.
 - d) Click **Save**.
-

What to do next

After configuring the necessary settings for the network profile, click **Save**. For more information, see [Create Network Profiles for Wireless, on page 281](#).



PART **IV**

Configure and Maintain Network Devices

- [Create Templates to Automate Device Configuration Changes, on page 291](#)
- [Design Model Configuration, on page 313](#)
- [Manage Software Images, on page 331](#)
- [Compliance Audit for Network Devices, on page 349](#)
- [Run Diagnostic Commands on Devices, on page 361](#)



CHAPTER 11

Create Templates to Automate Device Configuration Changes

- [About Template Hub, on page 291](#)
- [Create Projects, on page 293](#)
- [Create Templates, on page 293](#)
- [Export Template\(s\), on page 298](#)
- [Import Template\(s\), on page 299](#)
- [Clone a Template, on page 299](#)
- [Attach a CLI Template to the Network Profiles, on page 300](#)
- [Provision CLI Templates, on page 301](#)
- [Export Project\(s\), on page 301](#)
- [Import Project\(s\), on page 301](#)
- [Template Variables, on page 302](#)
- [Associate Templates to Network Profiles, on page 309](#)
- [Detect Conflicts in a CLI Template, on page 310](#)

About Template Hub

Cisco DNA Center provides an interactive template hub to author CLI templates. You can design templates easily with a predefined configuration by using parameterized elements or variables. After creating a template, you can use the template to deploy your devices in one or more sites that are configured anywhere in your network.

With Template Hub, you can:

- View the list of available templates.
- Create, edit, clone, import, export, and delete a template.
- Filter the template based on the **Project Name**, template **Type**, **Template Language**, **Category**, **Device Family**, **Device Series**, **Commit State** and **Provision Status**.
- View the following attributes of the template in the **Template Hub** window, under the **Templates** table:
 - **Name**: Name of the CLI template.
 - **Project**: Project under which the CLI template is created.

- **Type:** Type of CLI template (regular or composite).
- **Version:** Number of versions of the CLI template.
- **Commit State:** Shows if the latest version of the template is committed. You can view the following information under the **Commit State** column:
 - The timestamp of the last committed date.
 - A warning icon means the template is modified but not committed.
 - A check icon means the latest version of the template is committed.



Note The last template version must be committed to provision the template on the devices.

- **Provision Status:** You can view the following information under the **Provision Status** column:
 - The count of devices on which the template is provisioned.
 - A check icon displays the count of devices for which the CLI template was provisioned without any failures.
 - A warning icon displays the count of devices for which the latest version of the CLI template is not yet provisioned.
 - A cross icon displays the count of devices for which the CLI template deployment failed.
 - **Potential Design Conflicts:** Displays potential conflicts in the CLI template.
 - **Network Profiles:** Displays the number of network profiles to which a CLI template is attached. Use the link under the **Network Profiles** column to attach a CLI template to network profiles.
 - **Actions:** Click the ellipsis under the **Actions** column to clone, commit, delete, or edit a template; edit a project; or attach a template to a network profile.
- Attach templates to network profiles. For more information, see [Attach a CLI Template to the Network Profiles, on page 300](#).
 - View the number of network profiles to which a CLI template is attached.
 - Add interactive commands.
 - Autosave the CLI commands.
 - Version control the templates for tracking purposes.
- You can view the versions of a CLI template. In the **Template Hub** window, click the template name and click the **Template History** tab to view the template version.
- Detect errors in templates.
 - Simulate templates.
 - Define variables.

- Detect potential design conflict and run-time conflict.



Note Be careful that your template does not overwrite a network-intent configuration pushed by Cisco DNA Center.

Create Projects

Step 1 Click the menu icon (☰) and choose **Tools > Template Hub**.

Step 2 Click **Add** at the top right corner of the window and choose, **New Project** from the drop-down list.

The **Add New Project** slide-in pane is displayed.

Step 3 Enter a unique name in the **Project Name** field.

Step 4 (Optional) Enter a description for the project in the **Project Description** field.

Step 5 Click **Continue**.

The project is created and appears in the left pane.

What to do next

Add new template to the project. For more information, see [Create a Regular Template, on page 293](#) and [Create a Composite Template, on page 295](#).

Create Templates

Templates provide a method to easily predefine configurations using parameter elements and variables. Templates allow an administrator to define a configuration of CLI commands that can be used to consistently configure multiple network devices, reducing deployment time. Variables in the template allow customization of specific settings per device.

Create a Regular Template

Step 1 Click the menu icon (☰) and choose **Tools > Template Hub**.

Note By default, the **Onboarding Configuration** project is available for creating day-0 templates. You can create your own custom projects. Templates created in custom projects are categorized as day-N templates.

Step 2 In the left pane, click **Project Name** and select the project under which you are creating templates.

Step 3 Click **Add** at the top right of the window, and choose **New Template** from the drop-down list.

Note The template that you create for day-0 can also be applied for day-N.

Step 4 In **Add New Template** slide-in pane, configure the settings for the regular template.

In the **Template Details** area do the following:

- a. Enter a unique name in the **Template Name** field.
- b. Choose the **Project Name** from the drop-down list.
- c. **Template Type**: Click **Regular Template** radio button.
- d. **Template Language**: Choose either the **Velocity** or **Jinja** language to be used for the template content.
 - **Velocity**: Use the Velocity Template Language (VTL). For information, see <http://velocity.apache.org/engine/devel/vtl-reference.html>.
 The Velocity template framework restricts the use of variables that start with a number. Make sure that the variable name starts with a letter and not with a number.

Note Do not use the dollar (\$) sign while using the velocity templates. If you have used the dollar (\$) sign, any value behind it is treated as a variable. For example, if a password is configured as "\$a123\$q1ups1\$va112", then the Template Hub treats this as variables "a123", "q1ups", and "va112". To workaround this issue, use Linux shell style for text processing with Velocity templates.

Note Use the dollar (\$) sign in the velocity templates only when declaring a variable.
 - **Jinja**: Use the Jinja language. For information, see <https://www.palletsprojects.com/p/jinja/>.
- e. Choose the **Software Type** from the drop-down list.

Note You can select the specific software type (such as IOS-XE or IOS-XR) if there are commands specific to these software types. If you select IOS as the software type, the commands apply to all software types, including IOS-XE and IOS-XR. This value is used during provisioning to check whether the selected device confirms to the selection in the template.

In the **Device Type Details** area do the following:

- a. Click **Add Device Details** link.
- b. Choose **Device Family** from the drop-down list.
- c. Click the **Device Series** tab and check the check box next to the preferred device series.
- d. Click the **Device Models** tab and check the check box next to the preferred device model.
- e. Click **Add**.

In **Additional Details** area do the following:

- a. Choose the **Device Tags** from the drop-down list.

Note Tags are like keywords that help you locate your template more easily.

If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get the following error during provisioning:

```
Cannot select the device. Not compatible with template
```
- b. Enter the **Software Version** in the software version field.

Note During provisioning, Cisco DNA Center checks to see if the selected device has the software version listed in the template. If there is a mismatch, the template is not provisioned.

- c. Enter the **Template Description**.

Step 5 Click **Continue**.

The template is created and appears under the **Templates** table.

Step 6 You can edit the template content by selecting the template that you created, click the ellipsis under **Actions** column, and choose **Edit Template**. For more information about editing the template content, see [Edit Templates, on page 297](#).

Blocked List Commands

Blocked list commands are commands that cannot be added to a template or provisioned through a template. If you use blocked list commands in your templates, it shows a warning in the template that it may potentially conflict with some of the Cisco DNA Center provisioning applications.

The following commands are blocked in this release:

- **router lisp**
- **hostname**

Sample Templates

Refer to these sample templates for switches while creating variables for your template.

Configure Hostname

```
hostname $name
```

Configure Interface

```
interface $interfaceName  
description $description
```

Configure NTP on Cisco Wireless Controllers

```
config time ntp interval $interval
```

Create a Composite Template

Two or more regular templates are grouped into a composite sequence template. You can create a composite sequential template for a set of templates, which are applied collectively to devices. For example, when you deploy a branch, you must specify the minimum configurations for the branch router. The templates that you create can be added to a single composite template, which aggregates all the individual templates that you need for the branch router. You must specify the order in which templates that are in the composite template are deployed to devices.



Note You can add only a committed template to a composite template.

Step 1 Click the menu icon (☰) and choose **Tools > Template Hub**.

Step 2 In the left pane, click **Project Name** and select the project under which you are creating templates.

Step 3 Click **Add** at the top right of the window, and choose **New Template** from the drop-down list.

The **Add New Template** slide-in pane is displayed.

Step 4 In **Add New Template** slide-in pane, configure the settings for the composite template.

In the **Template Details** area do the following:

- a) Enter a unique name in the **Template Name** field.
- b) Choose the **Project Name** from the drop-down list.
- c) **Template Type**: Choose **Composite Sequence** radio button.
- d) Choose the **Software Type** from the drop-down list.

Note You can select the specific software type (such as IOS-XE or IOS-XR) if there are commands specific to these software types. If you select IOS as the software type, the commands apply to all software types, including IOS-XE and IOS-XR. This value is used during provisioning to check whether the selected device confirms to the selection in the template.

In the **Device Type Details** area do the following:

- a. Click **Add Device Details** link.
- b. Choose **Device Family** from the drop-down list.
- c. Click the **Device Series** tab and check the check box next to the preferred device series.
- d. Click the **Device Models** tab and check the check box next to the preferred device model.
- e. Click **Add**.

In **Additional Details** area do the following:

- a. Choose the **Device Tags** from the drop-down list.

Note Tags are like keywords that help you locate your template more easily.

If you use tags to filter the templates, you must apply the same tags to the device to which you want to apply the templates. Otherwise, you get the following error during provisioning:

```
Cannot select the device. Not compatible with template
```

- b. Enter the **Software Version** in the software version field.

Note During provisioning, Cisco DNA Center checks to see if the selected device has the software version listed in the template. If there is a mismatch, the template is not provisioned.

- c. Enter the **Template Description**.

- Step 5** Click **Continue**.
The composite template window is displayed, which shows the list of applicable templates.
- Step 6** Click **Add Templates** link and click **+** to add the templates and click **Done**.
The composite template is created.
- Step 7** Check the check box next to the composite template that you created, click the ellipsis under **Actions** column, and choose **Commit** to commit the template content.
-


Edit Templates

After creating a template, you can edit the template to include content.

- Step 1** Click the menu icon (☰) and choose **Tools > Template Hub**.
- Step 2** In the left pane, choose the **Project Name** and select the template that you want to edit.
The chosen template is displayed.
- Step 3** Enter the template content. You can have a template with a single-line configuration or a multi-select configuration.
- Step 4** Click **Properties** next to the template name at the top of the window to edit **Template Details**, **Device Details** and **Additional Details**. Click **Edit** next to the respective area.
- Step 5** The template is auto saved. You can also choose to change the time interval of auto save, by clicking at the time recurrence next to **Auto Saved**.
- Step 6** Click **Template History** to view the versions of the template. Also, you can click **Compare** to view the difference in the template versions.
- Step 7** Click **Variables** tab to view the variables from the CLI template.
- Step 8** Click the **Show Design Conflicts** toggle button to view potential errors in the template.
Cisco DNA Center allows you to view, potential and run-time errors. For more information, see [Potential Design Conflicts Detection Between CLI Template and Service Provisioning Intent, on page 311](#) and [Detect CLI Template Run-Time Conflict, on page 311](#).
- Step 9** Click **Save** at the bottom of the window.
After saving the template, Cisco DNA Center checks for any errors in the template. If there are any syntax errors, the template content is not saved and all input variables that are defined in the template are automatically identified during the save process. The local variables (variables that are used in **for** loops, assigned though a set, and so on) are ignored.
- Step 10** Click **Commit** to commit the template.
Note You can associate only a committed template to a network profile.
- Step 11** Click **Attach to Network Profile** link, to attach the created template to a network profile.
-


Template Simulation

The interactive template simulation lets you simulate the CLI generation of templates by specifying test data for variables before sending them to devices. You can save the test simulation results and use them later, if required.

-
- Step 1** Click the menu icon () and choose **Tools > Template Hub**.
- Step 2** From the left pane, choose a project and click a template, for which you want to run a simulation.
The template is displayed.
- Step 3** Click the **Simulation** tab.
- Step 4** Click **Create Simulation**.
The **Create Simulation** slide-in pane is displayed.
- Step 5** Enter a unique name in **Simulation Name** field.
- Note** If there are implicit variables in your template then select a device from the **Device** drop-down list to run the simulation against real devices based on your bindings.
- Step 6** Click **Import Template Parameters** to import the template parameters or click **Export Template Parameters** to export the template parameters.
- Step 7** To use the variables from the last device provisioning, click **Use Variable Values from the Last Provisioning** link.
New variables must be added manually.
- Step 8** Choose values of the variables, by clicking on the link and click **Run**.
-

Export Template(s)

You can export a template or multiple templates to a single file, in JSON format.

- Step 1** Click the menu icon () and choose **Tools > Template Hub**.
- Step 2** Check a check box or multiple check box, next to the template name to select a template or multiple template that you want to export.
- Step 3** From the **Export** drop-down list, choose **Export Template**.
- Step 4** (Optional) You can filter the templates based on categories in the left pane.
- Step 5** The latest version of the template is exported.
To export an earlier version of the template, do the following:
- a. Click the template name to open the template.
 - b. Click **Template History** tab.
The **Template History** slide-in pane is displayed.
 - c. Choose the preferred version.
 - d. Click **View** button below the version.
The CLI template of that version is displayed.
 - e. Click **Export** at the top of the template.

The JSON format of the template is exported.

Import Template(s)

You can import a template or multiple templates under a project.



Note You can import templates only from an earlier version of Cisco DNA Center to a newer version. However, the opposite is not allowed.

Step 1 Click the menu icon (☰) and choose **Tools > Template Hub**.

Step 2 In the left pane, choose the project for which you want to import templates, under **Project Name** and choose **Import > Import Template**.

Step 3 **Import Templates** slide-in pane is displayed.

- a. Choose the **Project Name** from the drop-down list.
- b. Upload the JSON file by doing one of the following actions:
 1. Drag and drop the file to the drag and drop area.
 2. Click, **Choose a file**, browse to the location of the JSON file, and click **Open**.

File size should not exceed 10Mb.

- c. Check the check box to create a new version of imported template, if template with the same name already exists in the hierarchy.
- d. Click **Import**.

The CLI template is successfully imported to the chosen project.

Clone a Template

You can make a copy of a template to reuse portions of it.

Step 1 Click the menu icon (☰) and choose **Tools > Template Hub**.

Step 2 Click the ellipsis under **Action** column and choose **Clone**.

Step 3 The **Clone Template** slide-in pane is displayed.

Do the following:

- a. Enter a unique name in **Template Name** field.

- b. Choose the **Project Name** from the drop-down list.

Step 4 Click **Clone**.

The latest version of the template is cloned.

Step 5 (Optional) Alternatively, you can clone the template by clicking the template name. The template is displayed. Click **Clone** above the template.

Step 6 To clone an earlier version of the template, do the following:

- a. Select the template by clicking the template name.
- b. Click the **Template History** tab.
The **Template History** slide-in pane is displayed.
- c. Click the preferred version.
The chosen CLI template is displayed.
- d. Click **Clone** above the template.

Attach a CLI Template to the Network Profiles

To provision a CLI template, it needs to be attached to a network profile. Use this procedure to attach a CLI template to a network profile or multiple network profiles.

Step 1 Click the menu icon (☰) and choose **Tools > Template Hub**.

The **Template Hub** window is displayed.

Step 2 Click **Attach**, under **Network Profile** column, to attach the a template to the network profile.

Note Alternatively, you can click the ellipsis under **Actions** column and choose **Attach to Profile** or you can attach a template to network profile from **Design > Network Profiles**. For more information, see [Associate Templates to Network Profiles, on page 309](#).

Attach to Network Profile slide-in pane is displayed.

Step 3 Check the check box next to the network profile name and click **Save**.

The CLI Template is attached to the chosen Network Profile.

Step 4 A number is displayed under **Network Profile** column, which shows the number of network profiles to which a CLI template is attached. Click the number to view the network profile details.

Step 5 To attach more network profiles to a CLI template, do the following:

- a. Click the number under **Network Profile** column.
Alternatively, you can click the ellipsis under **Actions** column and choose **Attach to Profile**.
The **Network Profiles** slide-in pane is displayed.

- b. Click **Attach to Network Profile** link at the top right of the slide-in pane and check the check box next to the Network Profile name and click **Attach**.
-

Provision CLI Templates

- Step 1** Click the menu icon (☰) and choose **Tools > Template Hub**.
 - Step 2** Check the check box next to the template you want to provision and click **Provision Templates** at the top of the table.
You can choose to provision multiple templates.
You are redirected to the **Provision Template** workflow.
 - Step 3** In the **Get Started** window, enter a unique name in **Task Name** field.
 - Step 4** In the **Select Devices** window, choose the devices from the applicable devices list, which are based on the device details defined in the template and click **Next**.
 - Step 5** In the **Review Applicable Templates** window, review the devices and the templates attached to it. If required, you can remove the templates that you do not want to be provisioned on the device.
 - Step 6** Configure the template variables for each device, in **Configure Template Variables** window.
 - Step 7** Select the device to preview the configuration being provisioned on the device, in **Preview Configuration** window.
 - Step 8** In the **Schedule Task** window, select whether to provision the template **Now**, or schedule the provision for a **Later** time, and click **Next**.
 - Step 9** In the **Summary** window, review the template configurations for your devices, click **Edit** to make any changes; otherwise click **Submit**.
Your devices will be provisioned with the template.
-

Export Project(s)

You can export a project or multiple projects, including their templates, to a single file in JSON format.

- Step 1** Click the menu icon (☰) and choose **Tools > Template Hub**.
 - Step 2** In the left pane, select a project or multiple project that you want to export under **Project Name**.
 - Step 3** From **Export** drop-down list, choose **Export Project**.
 - Step 4** Click **Save**, if prompted.
-

Import Project(s)

You can import a project or multiple projects with their templates, into the Cisco DNA Center Template Hub.



Note You can import projects only from an earlier version of Cisco DNA Center to a newer version. However, the opposite is not allowed.

Step 1 Click the menu icon (☰) and choose **Tools > Template Hub**.

Step 2 From the **Import** drop-down list, choose **Import Project**.

Step 3 The **Import Projects** slide-in pane is displayed.

a. Upload the JSON file by doing one of the following actions:

1. Drag and drop the file to the drag and drop area.
2. Click **Choose a file**, browse to the location of the JSON file, and click **Open**.

File size should not exceed 10Mb.

b. Check the check box to create a new version of the template, in the existing project, if the project with the same name already exists in hierarchy.

c. Click **Import**.

The project is successfully imported.

Template Variables

The Template Variables is used for adding additional metadata information to the template variables in the template. You can also use the variables to provide validations for variables such as maximum length, range, and so on.

Step 1 Click the menu icon (☰) and choose **Tools > Template Hub**.

Step 2 From the left pane, choose a project and click a template.

The template is displayed.

Step 3 Click the **Variables** tab.

It enables you to add meta data to the template variables. All the variables that are identified in the template are displayed. You can configure the following metadata:

- Choose the variable from the left pane, and click the **Variable** toggle button if you want the string to be considered as a variable.

Note By default the string considered as a variable. Click the toggle button, if you do not want the string to be considered as a variable.

- Check the **Required Variable** check box if this is a required variable during the provisioning. All the variables by default are marked as Required, which means you must enter the value for this variable at the time of provisioning. If the parameter is not marked as **Required Variable** and if you do not pass any value to the parameter, it substitutes

an empty string at run time. A lack of a variable can lead to command failure, which may not be syntactically correct. If you want to make an entire command optional based on a variable not marked as **Required Variable**, use the **if-else** block in the template.

- Enter the field name in the **Field Name**. This is the label that is used for the UI widget of each variable during provisioning.
- In **Variable Data Value** area, choose the **Variable Data Source** by clicking the radio button. You can choose, **User Defined** value or **Bound to Source** value to hold a specific value.

Do the following, if you choose **User Defined** value:

- a. Choose the **Variable Type** from the drop-down list: **String**, **Integer**, **IP Address**, or **Mac Address**
- b. Choose the **Data Entry Type** from the drop-down list: **Text Field**, **Single Select**, or **Multi Select**.
- c. Enter the default variable value in the **Default Variable Value** field.
- d. Check the **Sensitive Value** check box for sensitive value.
- e. Enter the number of characters that are allowed in the **Maximum Characters** field. This is applicable only for the string data type.
- f. Enter hint text in the **Hint Text** field.
- g. Enter any additional information in the **Additional Info** text box.

Do the following, if you choose **Bound to Source** value:

- a. Choose the **Data Entry Type** from the drop-down list: **Text Field**, **Single Select**, or **Multi Select**.
- b. Choose the **Source** from the drop-down list: **Network Profile**, **Common Settings**, **Cloud Connect** and **Inventory**.
- c. Choose the **Entity** from the drop-down list.
- d. Choose the **Attribute** from the drop-down list.
- e. Enter the number of characters that are allowed in the **Maximum Characters** field. This is applicable only for the string data type.
- f. Enter hint text in the **Hint Text** field.
- g. Enter any additional information in the **Additional Info** text box.

For more details on **Bound to Source** value, see [Variable Binding, on page 303](#).

Step 4 After configuring metadata information, click **Review Form** to review the variable information.

Step 5 Click **Save**.

Step 6 To commit the template, choose **Commit**. The **Commit** window is displayed. You can enter a commit note in the **Commit Note** text box.

Variable Binding

While creating a template, you can specify variables that are contextually substituted. Many of these variables are available in the Template Hub.

Template Hub provides an option to bind or use variables in the template with the source object values while editing or through the input form enhancements; for example, DHCP server, DNS server, and syslog server.

Some variables are always bound to their corresponding source and their behavior cannot be changed. To view the list of implicit variables, click the template and click **Variables** tab.

The predefined object values can be one of the following:

- Network Profile
 - SSID
 - Policy profile
 - AP group
 - Flex group
 - Flex profile
 - Site tag
 - Policy tag
- Common Settings
 - DHCP server
 - Syslog server
 - SNMP trap receiver
 - NTP server
 - Timezone site
 - Device banner
 - DNS server
 - NetFlow collector
 - AAA network server
 - AAA endpoint server
 - AAA server pan network
 - AAA server pan endpoint
 - WLAN info
 - RF profile info
- Cloud Connect
 - Cloud router-1 Tunnel IP
 - Cloud router-2 Tunnel IP
 - Cloud router-1 Loopback IP

- Cloud router-2 Loopback IP
 - Branch router-1 Tunnel IP
 - Branch router-2 Tunnel IP
 - Cloud router-1 Public IP
 - Cloud router-2 Public IP
 - Branch router-1 IP
 - Branch router-2 IP
 - Private subnet-1 IP
 - Private subnet-2 IP
 - Private subnet-1 IP mask
 - Private subnet-2 IP mask
- Inventory
 - Device
 - Interface
 - AP group
 - Flex group
 - WLAN
 - Policy profile
 - Flex profile
 - Webauth parameter map
 - Site tag
 - Policy tag
 - RF profile
- **Common Settings:** Settings available under **Design > Network Settings > Network**. The common settings variable binding resolves values that are based on the site to which the device belongs.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Template Hub**.
- Step 2** Choose the template and click the **Variables** tab to bind variables in the template to network settings.
- Step 3** Select the variables in the left pane and check the **Required Variable** check box to bind variables to the network settings.
- Step 4** To bind variables to network settings, select each variable from the left pane, and choose **Bound to Source** radio button, under **Variable Data Source** and do the following:
- a. From the **Data Entry Type** drop-down list, choose the type of UI widget to create at the time of provisioning: **Text Field**, **Single Select**, or **Multi Select**.

- b. Choose the **Source**, **Entity**, and **Attribute** from the respective drop-down lists.
- c. For the source type **CommonSettings**, choose one of these entities: **dhcp.server**, **syslog.server**, **snmp.trap.receiver**, **ntp.server**, **timezone.site**, **device.banner**, **dns.server**, **netflow.collector**, **aaa.network.server**, **aaa.endpoint.server**, **aaa.server.pan.network**, **aaa.server.pan.endpoint**, **wlan.info** or **rfprofile.info**.

You can apply a filter on the **dns.server** or **netflow.collector** attributes to display only the relevant list of **bind** variables during provisioning of devices. To apply a filter on an attribute, select an attribute from the **Filter by** drop-down list. From the **Condition** drop-down list, select a condition to match the **Value**.

- d. For the source type **NetworkProfile**, choose **SSID** as the entity type. The SSID entity that is populated is defined under **Design > Network Profile**. The binding generates a user-friendly SSID name, which is a combination of SSID name, site, and SSID category. From the **Attributes** drop-down list, choose **wlanid** or **wlanProfileName**. This attribute is used during the advanced CLI configurations at the time of template provisioning.
- e. For the source type **Inventory**, choose one of these entities: **Device**, **Interface**, **AP Group**, **Flex Group**, **Wlan**, **Policy Profile**, **Flex Profile**, **Webauth Parameter Map**, **Site Tag**, **Policy Tag**, or **RF Profile**. For the entity type **Device** and **Interface**, the **Attribute** drop-down list shows the device or interface attributes. The variable resolves to the AP Group and Flex Group name that is configured on the device to which the template is applied.

You can apply filter on the **Device**, **Interface**, or **Wlan** attributes to display only the relevant list of **bind** variables during provisioning of devices. To apply a filter on an attribute, select an attribute from the **Filter by** drop-down list. From the **Condition** drop-down list, select a condition to match the **Value**.

After binding variables to a common setting, when you assign templates to a wireless profile and provision the template, the network settings that you defined under **Network Settings > Network** appear in the drop-down list. You must define these attributes under **Network Settings > Network** at the time of designing your network.

Step 5 If the template contains variable bindings that bind to specific attributes and the template code accesses those attributes directly, you must do one of the following:

- Change the binding to the object instead of to the attributes.
- Update the template code to not access the attributes directly.

For example, if the template code is as follows, where **\$interfaces** binds to specific attributes, you must update the code as shown in the following example, or modify the binding to the object instead of to the attributes.

Old sample code:

```
#foreach ( $interface in $interfaces )
  $interface.portName
    description "something"
#end
```

New sample code:

```
#foreach ( $interface in $interfaces )
  interface $interface
    description "something"
#end
```

Special Keywords

All commands executed through templates are always in the **config t** mode. Therefore, you do not have to specify the **enable** or **config t** commands explicitly in the template.

Day-0 templates do not support special keywords.

Enable Mode Commands

Specify the `#MODE_ENABLE` command if you want to execute any commands outside of the `config t` command.

Use this syntax to add **enable mode** commands to your CLI templates:

```
#MODE_ENABLE
<<commands>>
#MODE_END_ENABLE
```

Interactive Commands

Specify `#INTERACTIVE` if you want to execute a command where a user input is required.

An interactive command contains the input that you must enter 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>` tags evaluate the text provided against what is seen on the device.

The Interactive question uses regular expressions to validate if the text received from the device is similar to the text entered. If the regular expressions entered in the `<IQ><R>` tags are found, then the interactive question passes and a part of the output text appears. This means that you need to enter a part of the question and not the entire question. Entering Yes or No between the `<IQ>` and `<R>` tags is sufficient but you must make sure that the text Yes or No appears in the question output from the device. The best way to do this is by running the command on the device and observing the output. In addition, you need to ensure that any regular expression metacharacters or newlines entered are used appropriately or avoided completely. The common regular expression metacharacters are `. () [] {} | * + ? \ $ ^ : &`.

For example, the following command has output that includes metacharacters and newlines.

```
Switch(config)# no crypto pki trustpoint DNAC-CA
% Removing an enrolled trustpoint will destroy all certificates received from the related
Certificate Authority
Are you sure you want to do this? [yes/no]:
```

To enter this in a template, you need to select a portion that does not have any metacharacters or newlines. Here are a few examples of what could be used.

```
#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>yes/no<R>yes
#ENDS_INTERACTIVE
```

```
#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>Removing an enrolled<R>yes
#ENDS_INTERACTIVE
```

```
#INTERACTIVE
no crypto pki trustpoint DNAC-CA<IQ>Are you sure you want to do this<R>yes
#ENDS_INTERACTIVE
```

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Where **<IQ>** and **<R>** tags are case-sensitive and must be entered in uppercase.



Note In response to the interactive question after providing a response, if the newline character is not required, you must enter the **<SF>** tag. Include one space before the **<SF>** tag. When you enter the **<SF>** tag, the **</SF>** tag pops up automatically. You can delete the **</SF>** tag because it is not needed.

For example:

```
#INTERACTIVE
config advanced timers ap-fast-heartbeat local enable 20 <SF><IQ>Apply(y/n)?<R>y
#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

#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Multiline Commands

If you want multiple lines in the CLI template to wrap, use the **MLTCMD** tags. Otherwise, the command is sent line by line to the device. To enter multiline 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>** are case-sensitive and must be in uppercase.
- The multiline commands must be inserted between the **<MLTCMD>** and **</MLTCMD>** tags.
- The tags cannot start with a space.
- The **<MLTCMD>** and **</MLTCMD>** tags cannot be used in a single line.

Associate Templates to Network Profiles

Before you begin

Before provisioning a template, ensure that the template is associated with a network profile and the profile is assigned to a site.

During provisioning, when the devices are assigned to specific sites, the templates associated with the site through the network profile appear in the advanced configuration.

Step 1 Click the menu icon (☰) and choose **Design > Network Profiles**, and click **Add Profile**.

The following types of profiles are available:

- **Assurance:** Click this to create an Assurance profile.
- **Firewall:** Click this to create a firewall profile.
- **Routing:** Click this to create a routing profile.
- **Switching:** Click this to create a switching profile.
 - Click the **Onboarding Templates** or **Day-N Templates**, as required.
 - In the **Profile Name** field, enter the profile name.
 - Click **+Add Template** and choose the device type, tag, and template from the **Device Type**, **Tag Name**, and **Template** drop-down lists.

If you do not see the template that you need, create a new template in Template Hub. See [Create a Regular Template, on page 293](#).
 - Click **Save**.
- **Telemetry Appliance:** Click this to create a Cisco DNA Traffic Telemetry Appliance profile.
- **Wireless:** Click this to create a wireless profile. Before assigning a wireless network profile to a template, ensure that you have created wireless SSIDs.
 - In the **Profile Name** field, enter the profile name.
 - Click **+ Add SSID**. The SSIDs that were created under **Network Settings > Wireless** are populated.
 - Under **Attach Template(s)**, from the **Template** drop-down list, choose the template that you want to provision.
 - Click **Save**.

Note You can view the Switching and Wireless profiles in the **Cards** and the **Table** view.

Step 2 The **Network Profiles** window lists the following:

- **Profile Name**
- **Type**
- **Version**
- **Created By**
- **Sites:** Click **Assign Site** to add sites to the selected profile.

- Step 3** For Day-N provisioning, choose **Provision > Network Devices > Inventory** and do the following:
- Check the check box next to the device name that you want to provision.
 - From the **Actions** drop-down list, choose **Provision**.
 - In the **Assign Site** window, assign a site to which the profiles are attached.
 - In the **Choose a Site** field, enter the name of the site to which you want to associate the controller, or choose from the **Choose a Site** drop-down list.
 - Click **Next**.
 - The **Configuration** window appears. In the **Managed AP Locations** field, enter the AP locations managed by the controller. You can change, remove, or reassign the site. This is applicable only for wireless profiles.
 - Click **Next**.
 - The **Advanced Configuration** window appears. The templates associated with the site through the network profile appear in the advanced configuration.
 - Check the **Provision these templates even if they have been deployed before** check box if you overwrote any configurations from intent in the template, and you want your changes to override. (This option is disabled by default.)
 - The **Copy running config to startup config** option is enabled by default, which means that after deploying the template configuration, **write mem** will be applied. If you don't want to apply the running config to the startup config, you must uncheck this check box.
 - Use the **Find** feature to quickly search for the device by entering the device name, or expand the templates folder and select the template in the left pane. In the right pane, select values for those attributes that are bound to the source.
 - To export the template variables into a CSV file while deploying the template, click **Export** in the right pane. You can use the CSV file to make necessary changes in the variable configuration and import it into Cisco DNA Center at a later time by clicking **Import** in the right pane.
 - Click **Next** to deploy the template.
 - Choose whether you want to deploy the template **Now** or schedule it for later. The **Status** column in the **Device Inventory** window shows **SUCCESS** after the deployment succeeds.
- Step 4** Click **Export Deployment CSV** to export template variables from all the templates in a single file.
- Step 5** Click **Import Deployment CSV** to import template variables from all the templates in a single file.
- Step 6** For Day-0 provisioning, choose **Provision > Plug and Play** and do the following:
- Choose a device from the **Actions** drop-down list, and choose **Claim**.
 - Click **Next** and in **Site Assignment** window, choose a site from the **Site** drop-down list.
 - Click **Next** and in **Configuration** window, choose the image and the Day-0 template.
 - Click **Next** and in the **Advanced Configuration** window, enter the location.
 - Click **Next** to view the **Device Details**, **Image Details**, **Day-0 Configuration Preview**, and **Template CLI Preview**.

Detect Conflicts in a CLI Template

Cisco DNA Center allows you to detect conflicts in a CLI template. You can view potential design conflicts and run-time conflicts for switching, SD-Access, or fabric.

Potential Design Conflicts Detection Between CLI Template and Service Provisioning Intent

Potential Design Conflicts identify the intent commands in the CLI template and flag them, if the same command is pushed by switching, SD-Access, or fabric. Intent commands are not recommended for use, because they are reserved to be pushed to the device, by Cisco DNA Center.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Template Hub**.
The **Template Hub** window is displayed.
- Step 2** In the left pane, click the **Project Name** from the drop-down list to view the CLI templates of the preferred project.
Note To view only the templates with conflicts, in the left pane, under **Potential Design Conflicts**, check the **Conflicts** check box.
- Step 3** Click the template name.
Alternatively, you can click the warning icon under the **Potential Design Conflicts** column. The total number of conflicts is displayed.
The CLI Template is displayed.
- Step 4** In the template, the CLI commands that have conflicts are flagged with a warning icon. Hover over the warning icon to view the details of the conflict.
For new templates, the conflicts are detected after you save the template.
- Step 5** (Optional) To show or hide the conflicts, click the **Show Design Conflicts** toggle.
- Step 6** Click the menu icon (☰) and choose **Provision > Inventory** to view the number of CLI templates with conflicts. In the **Inventory** window a message with a warning icon is displayed, which shows the number of conflicts in the newly configured CLI template. Click the **Update CLI Templates** link to view the conflicts.
-

Detect CLI Template Run-Time Conflict

Cisco DNA Center allows you to detect run-time conflict for switching, SD-Access, or fabric.

Before you begin

You must configure the CLI template through Cisco DNA Center to detect run-time conflict.


-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
The **Inventory** window is displayed.
- Step 2** View the template provisioning status of devices under the **Template Provision Status** column, which shows the number of templates provisioned for the device. The templates that are provisioned successfully are displayed with a tick icon. The templates that have conflicts are displayed with a warning icon.
- Step 3** Click the link under the **Template Provision Status** column to open the **Template Status** slide-in pane.

You can view the following information in the table:

- **Template Name**
- **Project Name**
- **Provision Status:** Displays **Template Provisioned** if the template was provisioned successfully or **Template Out of Sync** if there are any conflicts in the template.
- **Conflict Status:** Displays the number of conflicts in the CLI template.
- **Actions:** Click **View Configuration** to view the CLI template. Commands that have conflicts are flagged with a warning icon.

Step 4 (Optional) View the number of conflicts in a CLI template under the **Template Conflicts Status** column in the **Inventory** window.

Step 5 Identify the run-time conflicts by generating a configuration preview:

- a) Check the check box next to the device name.
 - b) From the **Actions** drop-down list, choose **Provision Device**.
 - c) In the **Assign Site** window, click **Next**. In the **Advanced Configuration** window, make the necessary changes and click **Next**. In the **Summary** window, click **Deploy**.
 - d) In the **Provision Device** slide-in pane, click the **Generate Configuration Preview** radio button and click **Apply**.
 - e) Click the **Work Items** link to view the generated configuration preview. Alternatively, click the menu icon () and choose **Activities > Work Items** to view the generated configuration preview.
 - f) If the activity is still loading, click **Refresh**.
 - g) Click the preview link to open the **Configuration Preview** slide-in pane. You can view the CLI commands with run-time conflicts flagged with warning icons.
-



CHAPTER 12

Design Model Configuration

- [Introduction to Model Config Editor, on page 313](#)
- [Discover and Create Designs from a Legacy Device, on page 314](#)
- [Create a Model Config Design for AAA RADIUS Attributes, on page 314](#)
- [Create a Model Config Design for Advanced SSID, on page 315](#)
- [Create a Design for Cisco CleanAir, on page 319](#)
- [Create a Model Config Design for Dot11ax Configuration, on page 321](#)
- [Create a Model Config Design for Event-Driven RRM, on page 322](#)
- [Create a Design for Flex Configuration, on page 324](#)
- [Create a Design for Global IPv6, on page 326](#)
- [Create a Model Config Design for Multicast, on page 326](#)
- [Create a Model Config Design for RRM FRA Parameters, on page 328](#)
- [Create a Model Config Design for RRM General Parameters, on page 329](#)

Introduction to Model Config Editor

Model Config allows you to define advanced customizations of the Cisco Validated Designs (CVDs) that are encapsulated within the provisioning applications. Model Configs are a set of model-based, discoverable, and customizable configuration capabilities, which you can deploy on your network devices with high-level service intent and device-specific CLI templates.

The Model Configs feature simplifies network provision by extracting complex device configurations and facilitating customizable network configurations using an intuitive GUI instead of device-specific CLIs. A common design is deployed to various device hardware platforms and software types in a uniform way. During deployments, the Cisco DNA Center infrastructure automatically validates and translates extracted designs to device-specific CLI commands.

To provision model config design, do the following:

1. Create a new model config design using the **Model Config Editor** window (menu icon > **Tools** > **Model Config Editor**).
2. Apply the model config design to different network profiles.
3. Using the provision workflow, apply the model config design that is specified in network profiles to a network device.

Supported Model Config Design Types

Cisco DNA Center supports the following wireless Model Config design types:

- AAA Radius attributes configuration
- Advanced SSID configuration
- CleanAir configuration
- Event driven RRM configuration
- Flex configuration
- Dot11ax configuration
- Global IPv6 configuration
- Multicast configuration
- RRM FRA configuration
- RRM general configuration

Discover and Create Designs from a Legacy Device

Instead of manually creating designs using the Model Config Editor, you can use the Discover Model Configs feature to discover the existing model config designs available on legacy devices and use them as a template to create new designs.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** Click the **Discovery** tab.
- A list of discovered devices that are available in the **Inventory** window appears.
- Step 3** Click the radio button next to the device name and click **Discover Model Configs**.
- Step 4** In the right pane, expand **Wireless** and choose a model config design type.
- The configuration available for the selected model config type appears. For example, if you choose **CleanAir Configuration** under **Wireless**, the available configuration for the CleanAir appears.
- Step 5** Click the radio button next to the configuration that you want to use as a template to create a new design, and click **Create Design**.
- Step 6** In the window that appears, make the necessary changes and click **Save**.
-

Create a Model Config Design for AAA RADIUS Attributes

Use the **AAA Radius Attributes Configuration** model config to define the Called-station-id parameter value for Cisco AireOS Controllers and Cisco Catalyst 9800 Series Wireless Controllers.

The **Default AAA_Radius_Attributes_Configuration** defines the called-station ID as **ap-macaddress-ssid**. You cannot edit or delete this default model config. However, you can create a custom model config for your specific network design.

This procedure describes how to create a new AAA Radius Attributes Configuration model config.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search** field, or by expanding **Wireless** and choosing **AAA Radius Attributes Configuration**.
- Step 3** In the **Design Instances** window, click **Add**.
The **Add Called-station-id** slide-in pane appears.
- Step 4** In the **Design Name** field, enter a name for the model config design.
- Step 5** From the **Called-station-id** drop-down list, choose an attribute value.
- Step 6** Click **Save**.
The new design instance appears in the **Design Instances** window.
- Step 7** (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.
- Step 8** Attach the created config design to a network profile so that it can be deployed on a wireless controller. Click the menu icon (☰) and choose **Design > Network Profiles**.
For more information, see [Create Network Profiles for Wireless, on page 281](#).
- Step 9** Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
For more information, see [Provision a Cisco AireOS Controller, on page 391](#) or [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).
-

Create a Model Config Design for Advanced SSID

A WLAN associates an SSID to an interface or an interface group. The WLAN is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. You can configure up to 512 WLANs for each wireless controller.

Use the advanced service set identifier (SSID) model config to configure the advanced SSID parameters on devices.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search** field, or expand **Wireless** and choose **Advanced SSID Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default Advanced SSID Design** check box to use the default advanced SSID design.
- Note** You can't edit or delete the Default Advanced SSID Design.
- Step 4** In the **Design Instances** pane, click **Add Design**.
- Step 5** In the **Design Name** field of the **Add Advanced SSID Configuration** window, enter a name for the model config.
- Step 6** To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to the property.
- Step 7** In the **General** tab, click the **Peer-to-Peer Blocking** drop-down list and choose an option for peer-to-peer blocking. Peer-to-peer blocking is applied to individual WLANs. Each client inherits the peer-to-peer blocking setting of the WLAN to which it's associated. Peer-to-peer blocking enables you to have more control over how traffic is directed.
- **DISABLE**: Disables peer-to-peer blocking and forwards traffic locally within the wireless controller whenever possible.
 - **DROP**: Causes the wireless controller to discard the client packets.
 - **FORWARD UP**: Causes the client packets to be forwarded on an upstream VLAN. The device above the wireless controller decides what action to take regarding the packets. The device can either be a router or a Layer 3 switch.
 - **ALLOW PVT GROUP**: Applicable to preshared key (PSK) clients only. Traffic is forwarded based on the associated identity PSK (IPSK) tags for the source and destination client devices.
- Step 8** Click the **Passive Client Enable** toggle button to enable the Passive Client feature.
- Passive clients are wireless devices, such as scales and printers, that are configured with a static IP address. These clients do not transmit any IP information (such as IP address, subnet mask, and gateway information) when they associate with an access point. As a result, when passive clients are used, the wireless controller never knows the IP address unless they use DHCP.
- Step 9** Click the **Assisted Roaming Prediction Optimization** toggle button to configure an assisted roaming prediction list for a WLAN.
- Step 10** Click the **Neighbor List Dual Band** toggle button to configure a neighbor list on a dual radio band.
- Step 11** Click the **Network Admission Control (NAC-SNMP)** toggle button to enable SNMP NAC support on the WLAN.
- Step 12** Click the **Network Admission Control (NAC-Radius)** toggle button to enable RADIUS NAC support on the WLAN.
- Step 13** From the **DHCP Required** drop-down list, choose **Yes** or **No** to pass the DHCP request before going into the RUN state (a state where the client can pass traffic through the wireless controller).
- Step 14** Expand **DHCP Server** and enter the IP address of the DHCP server in the **IP Address** field.
- Step 15** Click the **FlexConnect Local Authentication** toggle button to enable FlexConnect local authentication.
- Step 16** Click the **802.11ax Status** toggle button to enable 802.11ax configuration parameters.

- Step 17** Click the **Aironet IE** toggle button to enable support for Aironet IE on this SSID.
- Step 18** Click the **Load Balance Enable** toggle button to enable the load balancing feature.
- Step 19** In the **DTIM Period 5GHz Band (In Beacon Intervals) [1-255]** field, enter a value for the 5GHz radio.
The valid range is from 1 through 255. The default value is 1 (to transmit broadcast and multicast frames after every beacon).
If the beacon period of the 802.11 network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames for 10 times every second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames for five times every second. Either of these settings are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.
However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon).
- Step 20** In the **DTIM Period 2.4GHz Band (In Beacon Intervals) [1-255]** field, enter a value for the 2.4GHz radio. The valid range is from 1 through 255. The default value is 1 (transmit broadcast and multicast frames after every beacon).
- Step 21** Set the time in milliseconds in the **Scan Defer Time [0-60000msecs]** field.
The valid values are between 0 and 60000 milliseconds; the default value is 100 milliseconds. If you set the time to 0, the scan deferral does not happen. The scan defer time is common for all priorities on the same WLAN and the scan is deferred if a packet is transmitted or received in any one of the defer priorities.
- Step 22** In the **Max Clients Per WLAN** field, enter the maximum number of clients that are allowed to join the WLAN.
The valid range is between 0 and 10000.
- Step 23** In the **Max Clients Per AP Radio Per WLAN [0-200]** field, enter the maximum number of clients that are allowed to join the WLAN per AP.
The valid range is between 0 and 200.
- Step 24** In the **Max Clients Per AP Radio Per WLAN [0-400]** field, enter the maximum number of client connections that are allowed per AP.
The valid range is between 0 and 400.
- Step 25** From the **WMM Policy** drop-down list, choose the WMM policy as **Allowed**, **Disabled**, or **Required**.
By default, the WMM policy is Allowed.
- Step 26** In the **NAS ID** field, enter the network access server identifier.
- Step 27** Click **Client Data Rates** to configure the following client data rate limits per client by entering values in the respective fields:
- Average Downstream Data Rate Per Client (kbps)
 - Burst Downstream Data Rate Per Client (kbps)
 - Average Downstream Real-Time Rate Per Client (kbps)
 - Burst Downstream Real-Time Rate Per Client (kbps)
 - Average Upstream Data Rate Per Client (kbps)
 - Burst Upstream Data Rate Per Client (kbps)
 - Average Upstream Real-Time Rate Per Client (kbps)

- Burst Upstream Real-Time Rate Per Client (kbps)

Step 28 Click the **SSID Data Rates** to configure the following SSID data rate limits per SSID by entering values in the respective fields:

- Average Upstream Data Rate Per SSID (kbps)
- Burst Upstream Data Rate Per SSID (kbps)
- Average Upstream Real-Time Rate Per SSID (kbps)
- Burst Upstream Real-Time Rate Per SSID (kbps)
- Average Downstream Data Rate Per SSID (kbps)
- Burst Downstream Data Rate Per SSID (kbps)
- Average Downstream Real-Time Rate Per SSID (kbps)
- Burst Downstream Real-Time Rate Per SSID (kbps)

Note To lock all the properties in the design, click **Lock all**. To lock a specific property, click the lock symbol next to that property.

Step 29 Hover your cursor over **More** and click **802.11ax Configuration** to configure the 802.11ax BSS configuration parameters. You can use the toggle button to enable or disable the following parameters:

- BSS Target Wake Up Time
- Downlink OFDMA
- Uplink OFDMA
- Downlink MU-MIMO
- Uplink MU-MIMO

Note These parameters apply only to 2.4-GHz and 5-GHz radio bands. You can configure 802.11ax parameters for the 6-GHz radio band under the **Wireless Radio Frequency Profile** section in the **Design > Network Settings > Wireless** window.

Step 30 Click **Save**.

The created design instance is displayed in the **Design Instances** window under the **Advanced SSID Configuration - Model Configs** area.

Step 31 To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

Step 32 Attach the created config design to a network profile so that it can be deployed on the wireless controller. Click the menu icon (☰) and choose **Design > Network Profiles**.

For more information, see [Create Network Profiles for Wireless, on page 281](#).

Step 33 Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

For more information, see [Provision a Cisco AireOS Controller, on page 391](#).

Create a Design for Cisco CleanAir

CleanAir is a spectrum intelligence solution designed to proactively manage the challenges of a shared wireless spectrum. It allows you to see all the users of the shared spectrum (both native devices and foreign interferers). It also enables you or your network to act on this information. For example, you can manually remove the interfering device, or the system can automatically steer the channel away from the interference. CleanAir provides spectrum management and Radio Frequency (RF) visibility.

Before you begin

You should have discovered the devices in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.

- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config capability by entering its name in the **Search Capability** field, or by expanding the **Wireless Model Configs** and choosing **CleanAir Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default CleanAir 802.11a Design** or **Default CleanAir 802.11b Design** check box to use the default CleanAir design.
- Note** You cannot edit and delete the **Default CleanAir 802.11a Design** or **Default CleanAir 802.11b Design**.
- Step 4** In the **Design Instances** window, click **Add**.
The **Add CleanAir Configuration** window is displayed.
- Step 5** In the **Design Name** field, enter a name for the design.
- Step 6** From the **Radio Band** drop-down list, choose **2.4 GHz** or **5 GHz**.
- Step 7** Click the **CleanAir Enable** toggle button to enable the CleanAir functionality on the 2.4-GHz or 5-GHz radio band.
If the **CleanAir Enable** toggle button is enabled, click it to prevent the Cisco Wireless Controller from detecting spectrum interference.
- Step 8** Click the **CleanAir Device Reporting Enable** toggle button to enable the CleanAir system to report detected sources of interference, if any.
If the **CleanAir Device Reporting Enable** toggle button is enabled, click it to prevent the Cisco Wireless Controller from reporting interferers.
- Step 9** Click the **Persistent Device Propagation** toggle button to enable propagation of information about persistent devices that can be detected by CleanAir.
Persistent device propagation enables you to propagate information about persistent devices to the neighboring APs that are connected to the same Cisco Wireless Controller. Persistent interferers are present at the location, and interfere with WLAN operations even if they are not detectable at all times.
- Step 10** Expand **Enable Interferers Features** and check the check box next to the source of interference that needs to be detected and reported by the CleanAir system:

- Ble Beacon
- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform
- Jammer
- Microwave Oven
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- Video
- Wimax Fixed
- Wimax Mobile
- Xbox

Step 11 In the **CleanAir Description** field, enter a description.

Step 12 Click **Apply**.

The created design instance appears in the **Design Instances** window under the **CleanAir Configuration - Model Configs** area.

Step 13 To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

Step 14 Attach the created config design to a network profile so that it can be deployed on the wireless controller. Click the menu icon (☰) and choose **Design > Network Profiles**.

For more information, see [Create Network Profiles for Wireless, on page 281](#).

Step 15 Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

For more information, see [Provision a Cisco AireOS Controller, on page 391](#).

Create a Model Config Design for Dot11ax Configuration

The Cisco DNA Center Dot11ax Model Config feature configures Dot11ax parameters on devices.

Dot11ax configuration involves the 802.11ax wireless specifications standard, also known as High Efficiency (HE) Wireless. Dot11ax is a dual-band technology that uses 2.4-GHz, 5-GHz, and 6-GHz bands. You can configure Dot11ax configuration parameters only on Wi-Fi 6-supported Cisco Catalyst 9100 Series Access Points.



Note BSS color is used to identify an overlapping basic service set (OBSS). BSS configs are pushed on Wi-Fi 6-supported access points only. The Cisco Catalyst 9100 Series Access Points are the next-generation Wi-Fi 802.11ax access points, and ideal for high-density, high-definition applications.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

Step 1 Click the menu icon (☰) and choose **Tools > Model Config Editor**.

Step 2 In the left pane, you can either search for a model config by entering its name in the **Search** field, or by expanding **Wireless** and choosing **Dot11ax Configuration**.

Step 3 In the **Design Instances** window, to use the default DOT11ax designs, check the check box next to the required default designs:

- **Default Dot11ax 6-GHz Design**
- **Default Dot11ax 802.11a Design**
- **Default Dot11ax 802.11b Design**

Note You can't edit or delete the default Dot11ax designs.

Step 4 Click **Add Design**.

The **Add Dot11ax Configuration** window opens.

Step 5 In the **Design Name** field, enter a name for the model config design.

Step 6 Click the **BSS Color** toggle button to enable the BSS color functionality. The default value is disabled. BSS color functionality is supported on:

- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later
- Cisco Wireless Controllers that run Cisco IOS XE Release 17.1 and later

Step 7 Click the **Target Wakeup Time** toggle button to enable the target wake-up time. The default value is disabled. Target wake-up time is supported on:

- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later
- Cisco Wireless Controllers that run Cisco IOS XE Release 17.1 and later

- Step 8** Click the **Target Wakeup Time Broadcast** toggle button to enable the target wake-up time broadcast. The default value is disabled.
- Target wake-up time broadcast is supported on:
- Cisco AireOS Wireless Controllers that run Cisco AireOS Release 8.10 and later
 - Cisco Wireless Controllers that run Cisco IOS XE Release 17.3.1 and later
- Step 9** Click the **Multiple BSSID** toggle button to enable the multiple basic service set identifier (BSSID) functionality. The default value is disabled.
- Multiple BSSID is supported only on Cisco Wireless Controllers that run Cisco IOS XE Release 17.7.1 and later.
- Note** This toggle button is available only when you choose the **6 GHz** radio band.
- Step 10** From the **Radio Band** drop-down list, choose 2.4-GHz, 5-GHz, or 6-GHz radio band. The default value is disabled.
- Step 11** Click the **OBSS PD** toggle button to enable the Overlapping BSS Packet Detect (OBSS-PD) functionality.
- OBSS-PD is supported only on Cisco Wireless Controllers that run Cisco IOS XE Release 17.4 and later.
- Note** This toggle button is not available for the **6 GHz** radio band.
- Step 12** In the **Non-SRG OBSS PD Max Threshold (dbm)** field, enter a value for the non-Spatial Reuse Group (SRG) OBSS-PD maximum threshold, in dBm. The default value is -62 dBm.
- Non-SRG OBSS-PD is supported only on Cisco Wireless Controllers that run Cisco IOS XE Release 17.4 and later.
- Note** This toggle button is not available for the **6 GHz** radio band.
- Step 13** (Optional) To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock symbol next to each property.
- A property that is locked in the design can't be changed during the device provisioning.
- Step 14** Click **Save**.
- The created design instance is displayed in the **Design Instances** window under the **Dot11ax Configuration – Model Configs** area.
- Step 15** To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.
- Step 16** Attach the created model config design to a network profile so that it can be deployed on the access points. Click the menu icon (☰) and choose **Design > Network Profiles**. For more information, see [Create Network Profiles for Wireless](#).
- Step 17** Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**. For more information, see [Provision a Cisco AireOS Controller, on page 391](#).
-

Create a Model Config Design for Event-Driven RRM

The event-driven RRM model config feature configures event-driven RRM parameters for 2.4-GHz, 5-GHz, and 6-GHz radios.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search** field, or expand **Wireless** and choose **Event Driven RRM Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default Event Driven 2.4GHz Design** or **Default Event Driven 5 GHz Design** check box to use the default advanced SSID design.
- Note** You cannot edit or delete the Default Event Driven RRM Design.
- Step 4** In the **Design Instances** pane, click **Add Design**.
The **Add Event Driven RRM Configuration** slide-in window appears.
- Step 5** In the **Design Name** field, enter a name for the model config.
- Step 6** From the **Radio Band** drop-down list, select the radio band: **2.4GHz**, **5GHz**, or **6GHz**.
- Note** The 6-GHz radio band is not supported on Cisco AireOS Wireless Controllers.
Cisco Catalyst 9800 Series Wireless Controller version 17.6 and later support the 6-GHz radio band.
- Step 7** Click the **Event Driven RRM** toggle button to run RRM when CleanAir-enabled AP detects a significant level of interference.
- Step 8** From the **Sensitivity Threshold** drop-down list, choose the sensitivity threshold level at which you want the RRM to be triggered from the following options.
When the interference for the AP rises above the threshold level, RRM initiates a local dynamic channel assignment (DCA) run and changes the channel of the affected AP radio, if possible, to improve network performance.
- **Low**: Specifies the least sensitivity to non-Wi-Fi interference as indicated by the AQ value.
 - **Medium**: Specifies medium sensitivity to non-Wi-Fi interference as indicated by the AQ value.
 - **High**: Specifies the most sensitivity to non-Wi-Fi interference as indicated by the AQ value.
 - **Custom**: Specifies custom sensitivity to non-Wi-Fi interference as indicated by the AQ value. If you choose this option, you must specify a custom value in the **Custom Threshold [1-99]** field.
- Step 9** Click **Save**.
The created design instance appears in the **Design Instances** window under the **Event Driven RRM Configuration - Model Configs** area.
- Step 10** To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.
- Step 11** Attach the created config design to a network profile so that it can be deployed on the wireless controller. Click the menu icon (☰) and choose **Design > Network Profiles**.
For more information, see [Create Network Profiles for Wireless, on page 281](#).

Step 12 Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

For more information, see [Provision a Cisco AireOS Controller, on page 391](#).

Create a Design for Flex Configuration

Use the flex model config feature to configure the FlexConnect configuration on devices.

Before you begin

Using the Discovery feature, discover the devices in your network so that the discovered devices are listed in the Inventory window.

Step 1 Click the menu icon (☰) and choose **Tools > Model Config Editor**.

Step 2 In the left pane, you can either search for a model config capability by entering its name in the **Search Capability** field, or by expanding the **Wireless** Model Configs and choosing **Flex Configuration**.

Step 3 In the **Design Instances** pane, check the **Default Flex Configuration** check box to use the default FlexConnect design.

Note You cannot edit and delete the **Default Flex Configuration** design.

Step 4 In the **Design Instances** window, click **Add**.

The **Add CleanAir Configuration** window is displayed.

Step 5 In the **Design Name** field, enter a name for the design.

Step 6 From the **Radio Band** drop-down list, choose **2.4 GHz** or **5 GHz**.

Step 7 Click the **CleanAir Enable** toggle button to enable the CleanAir functionality on the 2.4-GHz or 5-GHz radio band.

If the **CleanAir Enable** toggle button is enabled, click it to prevent the Cisco Wireless Controller from detecting spectrum interference.

Step 8 Click the **CleanAir Device Reporting Enable** toggle button to enable the CleanAir system to report detected sources of interference, if any.

If the **CleanAir Device Reporting Enable** toggle button is enabled, click it to prevent the Cisco Wireless Controller from reporting interferers.

Step 9 Click the **Persistent Device Propagation** toggle button to enable propagation of information about persistent devices that can be detected by CleanAir.

Persistent device propagation enables you to propagate information about persistent devices to the neighboring APs that are connected to the same Cisco Wireless Controller. Persistent interferers are present at the location, and interfere with WLAN operations even if they are not detectable at all times.

Step 10 Expand **Enable Interferers Features** and check the check box next to the source of interference that needs to be detected and reported by the CleanAir system:

- Ble Beacon

- Bluetooth Paging Inquiry
- Bluetooth SCO ACL
- Generic Dect
- Generic TDD
- Generic Waveform
- Jammer
- Microwave Oven
- Motorola Canopy
- SI FHSs
- Spectrum 802.11 FH
- Spectrum 802.11 Non STD Channel
- Spectrum 802.11 Spec Inverted
- Spectrum 802.11 Super AG SuperAG
- Spectrum 802.15.4
- Video
- Wimax Fixed
- Wimax Mobile
- Xbox

Step 11 In the **CleanAir Description** field, enter a description.

Step 12 Click **Apply**.

The created design instance appears in the **Design Instances** window under the **CleanAir Configuration - Model Configs** area.

Step 13 To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.

Step 14 Attach the created config design to a network profile so that it can be deployed on the wireless controller. Click the menu icon (☰) and choose **Design > Network Profiles**.

For more information, see [Create Network Profiles for Wireless, on page 281](#).

Step 15 Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

For more information, see [Provision a Cisco AireOS Controller, on page 391](#).

Create a Design for Global IPv6

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search Capability** field, or expand **Wireless** and choose **Global IPV6 Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default Global IPv6 Design** check box to use the default global IPv6 design.
- Note** You cannot edit or delete the **Default Global IPv6 Design**.
- Step 4** In the **Design Instances** window, click **Add Design**.
The **Add Global IPV6 Configuration** window appears.
- Step 5** In the **Design Name** field, enter a name for the model config.
- Step 6** Click the **Global IPV6 Config** toggle button to enable IPv6 globally on devices.
- Step 7** Click **Apply**.
The created design instance appears in the **Design Instances** window under the **Global IPV6 Configuration - Model Config** area.
- Step 8** To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.
- Step 9** Attach the created config design to a network profile so that it can be deployed on the wireless controller. Click the menu icon (☰) and choose **Design > Network Profiles**.
For more information, see [Create Network Profiles for Wireless, on page 281](#).
- Step 10** Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
For more information, see [Provision a Cisco AireOS Controller, on page 391](#).
-

Create a Model Config Design for Multicast

Use the multicast model config feature to configure multicast parameters on devices.

If your network supports packet multicasting, you can configure the multicast method that the Cisco Wireless Controller uses. The wireless controller performs multicasting in one of these modes:

- **Unicast mode:** In this mode, the wireless controller unicasts every multicast packet to every access point associated to the wireless controller. This mode is not very efficient, but is required on networks that do not support multicasting.

- **Multicast mode:** In this mode, the wireless controller sends multicast packets to a CAPWAP multicast group. This method reduces the overhead on the wireless controller processor and shifts the work of packet replication to your network. This method is more efficient than the unicast method.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search Capability** field, or by expanding **Wireless** and choosing **Multicast Configuration**.
- Step 3** In the **Design Instances** pane, check the **Default Multicast Design** check box to use the default multicast design.
- Note** You cannot edit or delete the **Default Multicast Design**.
- Step 4** In the **Design Instances** window, click **Add Design**.
The **Add Multicast Configuration** window appears.
- Step 5** In the **Design Name** field, enter a name for the model config design.
- Step 6** Click the **Enable Global Multicast Mode** toggle button to configure sending multicast packets. The default value is disabled.
- Step 7** From the **AP Multicast Mode** drop-down list, choose **UNICAST** or **MULTICAST**.
- Choose **UNICAST** to configure the wireless controller to use the unicast method to broadcast packets.
 - Choose **MULTICAST** to configure the wireless controller to use the multicast method to broadcast packets to a CAPWAP multicast group.
- Step 8** Expand **IPV4 Multicast Group Address** and enter the IPv4 multicast address in the **IP Address** field.
- Step 9** Expand **IPV6 Multicast Group Address** and enter the IPv6 multicast address in the **IP Address** field.
- Step 10** Click **Apply**.
The created design instance appears in the **Design Instances** window under the **Multicast - Model Config** area.
- Step 11** To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.
- Step 12** Attach the created config design to a network profile so that it can be deployed on the wireless controller. Click the menu icon (☰) and choose **Design > Network Profiles**.
For more information, see [Create Network Profiles for Wireless, on page 281](#).
- Step 13** Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
For more information, see [Provision a Cisco AireOS Controller, on page 391](#).
-

Create a Model Config Design for RRM FRA Parameters

The **RRM FRA Configuration** model configuration design configures the Flexible Radio Assignment (FRA) parameters for Radio Resource Management (RRM) for 2.4-5 GHz and 5-6 GHz radio bands.

Before you begin

You must discover the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model configuration by entering its name in the **Search** field, or expand **Wireless** and choose **RRM FRA Configuration**.
- Step 3** In the **Design Instances** window, check the corresponding default FRA design check box to use the default design:
- **Default FRA 2.4-5GHz Design**
 - **Default FRA 5-6GHz Design**
- Note**
- You can't edit or delete the default FRA designs.
 - The 6-GHz radio band is not supported in Cisco AireOS Wireless Controllers.
 - The Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.6 and later support the 6-GHz radio band.
- Step 4** In the **Design Instances** pane, click **Add**.
- Step 5** In the **Add Flexible Radio Assignment (FRA) Configuration** slide-in pane, enter a name for the model configuration.
- Step 6** (Optional) To lock all the properties in the design, click **Lock all**. To lock a specific property, click the corresponding lock icon next to each property.
- A property that is locked in the design can't be changed during device provisioning.
- Step 7** From the **Radio Band** drop-down list, choose a radio band.
- Step 8** Click the **FRA Freeze** toggle button to enable the FRA freeze functionality. This functionality is disabled by default. Cisco Wireless Controllers that run Cisco IOS XE Release 17.6.1 and later support this functionality.
- Note** This toggle button is available only for the **2.4-5 GHz** radio band.
- Step 9** Click the **FRA Status** toggle button to enable the FRA status functionality. This functionality is enabled by default.
- Step 10** From the **FRA Interval** drop-down list, choose an FRA interval.
- Step 11** From the **FRA Sensitivity** drop-down list, choose an FRA sensitivity value.
- This parameter sets the FRA coverage overlap sensitivity.
- Note** This drop-down list is available only for the **2.4-5 GHz** radio band.
- Step 12** Click **Save**.

The created design instance is displayed in the **Design Instances** window in the **RRM FRA Configuration – Model Configs** area.

- Step 13** (Optional) To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.
- Step 14** Attach the created model configuration design to a network profile so that it can be deployed on the access points. Click the menu icon (☰) and choose **Design > Network Profiles**. For more information, see [Create Network Profiles for Wireless, on page 281](#).
- Step 15** Provision the model configuration design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**. For more information, see [Provision a Cisco AireOS Controller, on page 391](#) and [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).
-

Create a Model Config Design for RRM General Parameters

The Radio Resource Management (RRM) general configuration model config feature configures the RRM general parameters for 2.4-GHz, 5-GHz, and 6-GHz radios.

Before you begin

You should have discovered the devices in your network using the **Discovery** feature so that the discovered devices are listed in the **Inventory** window.

- Step 1** Click the menu icon (☰) and choose **Tools > Model Config Editor**.
- Step 2** In the left pane, you can either search for a model config by entering its name in the **Search** field, or expand **Wireless** and choose **RRM General Configuration**.
- Step 3** The **Design Instances** pane shows the following default RRM general configuration designs. You can check the respective default **RRM General Design** check box to use the default design.
- You cannot edit or delete the Default RRM General Design.
- Default RRM General 2.4 GHz Design
 - Default RRM General 5 GHz Design
 - Default RRM General 6 GHz Design
- Note** The 6-GHz radio band is not supported on Cisco AireOS Wireless Controllers.
- Note** Cisco Catalyst 9800 Series Wireless Controller 17.6 and later releases support the 6-GHz radio band.
- Step 4** In the **Design Instances** pane, click **Add Design**.
- The **Add RRM General Configuration** slide-in window appears.
- Step 5** To lock all the properties in the design, click **Lock all**. To lock a specific property, click the lock symbol next to that property.
- Step 6** In the **Design Name** field, enter a name for the model config.
- Step 7** In the **Radio Band** tab, choose the radio band from the **Radio Band** drop-down list: 2.4 GHz, 5 GHz, or 6 GHz.

- Step 8** In the **Threshold** tab, set the throughput threshold value for the radio band selected in the Throughput Threshold (1000-10000000 Bps) field.
- Step 9** In the **Monitoring** tab, configure the monitoring channels and neighbor discover type.
- From the **Monitoring Channels** drop-down list, choose one of the following options to specify the set of channels that the AP uses for RRM scanning. By default, the monitoring channel is set to Country.
 - **All**: RRM channel scanning occurs on all channels supported by the selected radio, which includes channels not allowed in the country of operation.
 - **Country**: RRM channel scanning occurs only on the data channels in the country of operation. This is the default value.
 - **DCA**: RRM channel scanning occurs only on the channel set used by the DCA algorithm.
 - From the **Neighbor Discover Type** drop-down list, choose the neighbor discovery type. By default, the mode is set to Transparent.
 - **Transparent**: Sets the neighbor discover type to transparent. Packets are sent as is.
 - **Protected**: Sets the neighbor discover type to protected. Packets are encrypted.
- Step 10** In the **Coverage** tab, click the **Global Coverage Hole Detection Enabled** toggle button to enable coverage hole detection. By default, this value is selected.
- If you enable coverage hole detection, the Cisco Wireless Controller automatically determines, based on data received from the APs, if any APs have clients that are potentially located in areas with poor coverage.
- Step 11** Click **Save**.
- The created design instance appears in the **Design Instances** window under the **RRM General Configuration - Model Configs** area.
- Step 12** To edit a design, check the check box next to the design name that you want to edit, and click **Edit**. Make the changes and click **Save**.
- Step 13** Attach the created config design to a network profile so that it can be deployed on the wireless controller. Click the menu icon (☰) and choose **Design > Network Profiles**.
- For more information, see [Create Network Profiles for Wireless, on page 281](#).
- Step 14** Provision the model config design specified in the network profile to network devices. Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- For more information, see [Provision a Cisco AireOS Controller, on page 391](#).
-



CHAPTER 13

Manage Software Images

- [About Image Repository, on page 331](#)
- [Integrity Verification of Software Images, on page 332](#)
- [View Software Images, on page 332](#)
- [Use a Recommended Software Image, on page 335](#)
- [Import a Software Image, on page 335](#)
- [Assign a Software Image to a Device Family, on page 336](#)
- [Upload Software Images for Devices in Install Mode, on page 337](#)
- [About Golden Software Images, on page 337](#)
- [Specify a Golden Software Image, on page 338](#)
- [Configure an Image Distribution Server, on page 339](#)
- [Add Image Distribution Servers to Sites, on page 340](#)
- [Provision a Software Image, on page 341](#)

About Image Repository

Cisco DNA Center stores all the software images, software maintenance updates (SMUs), subpackages, ROMMON images, and so on, for the devices in your network. Image Repository provides the following functions:

- **Image Repository:** Cisco DNA Center stores all the unique software images according to image type and version. You can view, import, and delete software images.
- **Provision:** You can push software images to the devices in your network.

Before using Image Repository features, you must enable Transport Layer Security protocol (TLS) on older devices such as Cisco Catalyst 3000, 4000, and 6000. After any system upgrades, you must re-enable TLS. For more information, see “Configure Security for Cisco DNA Center” in the [Cisco DNA Center Administrator Guide](#).



Note In Release 2.3.3 and later, Cisco DNA Center supports only internal bootflash as the primary boot option for Software Image Management (SWIM) and Software Maintenance Updates (SMUs) on the IE3x00 series, and IE9x00 series switches.

If you have an earlier release of Cisco DNA Center (before Release 2.3.3), and if an IE3x00, or IE9x00 device in your network is already booted with a Secure Digital (SD) flash memory module, then ensure that you set the internal bootflash as the primary boot option on the device, using the **boot flash-primary** command.

To save and synchronize a running configuration from SD flash to bootflash, use the **sync** command.


Integrity Verification of Software Images

The Integrity Verification application monitors software images that are stored in Cisco DNA Center for unexpected changes or invalid values that could indicate your devices are compromised. During the import process, the system determines image integrity by comparing the software and hardware platform checksum value of the image that you are importing to the checksum value identified for the platform in the Known Good Values (KGV) file to ensure that the two values match.

On the **Image Repository** window, a message displays if the Integrity Verification application cannot verify the selected software image using the current KGV file. For more information about the Integrity Verification application and importing KGV files, see the [Cisco DNA Center Administrator Guide](#).

View Software Images

After you run Discovery or manually add devices, Cisco DNA Center automatically stores information about the software images, SMUs, and subpackages for the devices.

Step 1 Click the menu icon () and choose **Design > Image Repository**.

The **Image Repository** window summarizes the details about device families, software images, and advisories.

- **SUMMARY:** Shows the number of device families, devices, and device families without golden images in image repository.
- **TOTAL IMAGES:** Shows the number of running images, imported images, and golden images in image repository.
- **ADVISORIES:** Shows the number of critical and high advisories.

The **Image Families** table shows the details of **Family Name**, **Devices**, **Images**, **Advisories**, and **Images Marked Golden** for each device family.

Note When cisco.com credentials are not set, a warning alert is displayed.

Step 2 Click **Routers**, **Switches**, **Wireless Controllers**, **Security and VPN**, **Sensors**, or **Virtual Devices** in the top of the window or click the search or filter icon in the **Image Families** table to filter device families.

By default, the **Image Repository** window shows all the device families.

- Step 3** Click **Sync Updates** and then click **OK** in the subsequent warning message to synchronize image information from cisco.com for all managed devices in Cisco DNA Center.
- If cisco.com credentials are not set, you are prompted to specify them.
- You can view the progress of task in **Show Tasks**. Once the task is successful, the image information is updated for all device families.
- Note** You can fetch image information only once in an hour.
- Step 4** Click **Show Tasks** to view status of all the tasks that are related to software images.
- The **Recent Tasks** slide-in pane shows status of the last 50 tasks. From the **Task Status** drop-down list, choose **All**, **Failed**, **In-Progress**, or **Successful** to filter the tasks based on status.
- Step 5** Click **Import Image** to import a software image or software image update. For more information, see [Import a Software Image, on page 335](#).
- Step 6** Click **Update Devices** to update a device in inventory.
- In the **Inventory** window, choose a device and go to **Actions > Inventory** to edit, resync, reboot, or delete a device in inventory.
- Step 7** In the **Image Families** table, click **Imported Images** to view the details about imported software images. The **Imported Images** row is always displayed as the first row in the table.
- In the **Imported Image Family** window, the **Images** table shows **Image Name**, **Version**, **Device Series Assigned**, and **Action** for all the imported software images.
- In the **Action** column, click **Assign** to assign a software image to a device family. For more information, see [Assign a Software Image to a Device Family, on page 336](#).
- Step 8** In the **Image Families** table, click the name of a device family to view all the software images associated with the particular device family.
- In the **Image Family** window, the **Images** table shows the **Image Name**, **Version**, **Devices**, **Advisories**, **Golden Image**, **Device Roles & Tags** for all the software images.
- In the **Image Family** window, do the following:
- In the left pane, click **Roles & Tags**, **Major Versions**, or **Golden Images** or click the search or filter icon in the **Images** table to filter the software images.
 - In the **Version** column, click the **Add On** link to view the applicable **SMUs**, **Subpackages**, **ROMMON**, **APSP**, and **APDP** upgrades for the base image.
- Subpackages are the additional features that can be added to the existing base image. The subpackage version that matches the image family and the base image version is displayed here.
- AP Service Pack (APSP) and AP Device Pack (APDP) are images for upgrading APs associated with wireless controllers.
- When a new AP hardware model is introduced, APDP is used to connect to the existing wireless network.
 - For associated APs, critical AP bug fixes are applied through APSP.

Note If you tag any SMU as golden, it is automatically activated when the base image is installed. You cannot tag a subpackage as golden.

For ROMMON upgrades, the cisco.com configuration is mandatory. When a device is added, the latest ROMMON details are retrieved from cisco.com for applicable devices. Also, when the base image is imported or tagged, the ROMMON image is automatically downloaded from cisco.com.

- c) In the **Device(s)** column, click the number of devices to view the devices that are using the image.
- d) In the **Advisory** column, click the number of critical or high advisories to view the advisories for a specific software image.

The **Image Advisory** slide-in pane shows **Family Name**, **Version**, and **Advisories** of the software image. The advisories are classified as **Critical**, **High**, **Medium**, **Low**, and **Informational**.

Click **CRITICAL**, **HIGH**, or **MEDIUM** to view the advisories specific to each category.

To fix the advisories, do the following:

1. Click Fix Advisories.

The **Image Update** window appears.

2. Select a recommended software image to update the device.

If the recommended software image is not available in the image repository, you can download it from cisco.com.

3. Click Download and Mark Golden.

From the **Download Image** dialog box, do one of the following:

- Keep the **Mark the image as golden after download** check box checked (the default). Then, click **Download**. The software image is downloaded and marked as golden.
- Uncheck the **Mark the image as golden after download** check box and click **Download**. The software image is downloaded to the repository but is not marked as golden.

4. Click OK.

The software image is downloaded. You can view the progress in **Show Tasks**.

- e) In the **Golden Image** column, click the star icon to specify the software image as golden.

If the software image that you specify as golden is not already uploaded into the Cisco DNA Center repository, click the download icon to import the software image.

For more information about golden images, see [About Golden Software Images, on page 337](#) and [Specify a Golden Software Image, on page 338](#).

- f) In the **Device Roles & Tags** column, do the following:

1. Click the edit icon to assign a device role or tag.

To assign a device role and/or tag, the corresponding software image must have been imported.

2. In the Assign Device Roles & Tags slide-in pane, select the device roles and tags for which you want to indicate that this is a golden software image.

- Note**
- Device tags take precedence over device roles when both are selected for a software image.
 - You can create and assign new device tags in **Provision > Network Devices > Inventory**.

3. Click **Save**.

Use a Recommended Software Image

Cisco DNA Center displays and allows you to select Cisco-recommended software images for the devices that it manages.



Note Only the latest Cisco-recommended software images are available for download.

-
- Step 1** Click the menu icon (☰) and choose **System > Settings > Cisco.com Credentials**.
- Step 2** Verify that you have entered the correct credentials to connect to cisco.com.
- Step 3** Click the menu icon (☰) and choose **Design > Image Repository**.
Cisco DNA Center displays the Cisco-recommended software images according to device type.
- Step 4** Designate the recommended image as golden. See [Specify a Golden Software Image, on page 338](#) for more information.
- Step 5** Push the recommended software image to the devices in your network. See [Provision a Software Image, on page 341](#) for more information.
-

Import a Software Image

You can import software images and software image updates from your local computer or from a URL.

Imported images are categorized based on different supervisors that are present in a specific device family. Categorization under different supervisors supports only the Cisco Catalyst 9400 series family.

If you use FTP to import an image from an FTP server, use the FTP standard:

```
ftp://username:password@ip_or_hostname/path
```


-
- Step 1** Click the menu icon (☰) and choose **Design > Image Repository**.
- Step 2** Click **Import Image**.
- Step 3** In the **Import Image/Add-on** slide-in pane, click the **Select from computer** radio button and click **Choose a file** to navigate to a software image or software image update stored locally.
Alternately, click the **Enter URL** radio button and enter the image URL in the **Enter Image URL** field to specify an HTTP or FTP source from which you want to import the software image or software image updates.
- Note** Software images are compliant with Federal Information Processing Standard (FIPS). If FIPS mode is enabled in Cisco DNA Center, you cannot import images from URL. Import images from your computer or cisco.com.

- Step 4** If the image you are importing is for a third-party (non-Cisco) vendor, select **Third party** under **Source**. Choose an **Application Type**, describe the device **Family**, and identify the **Vendor**.
- Step 5** Click **Import**.
A window displays the progress of the import.
- Step 6** Click **Show Tasks** to verify that the image was imported successfully.
If you imported a SMU, Cisco DNA Center automatically applies the SMU to the correct software image, and an **Add-On** link appears below the corresponding software image.
- Step 7** Click the **Add-On** link to view the SMU.
- Step 8** In the **Device Role** field, select the role for which you want to mark this SMU as golden. See [Specify a Golden Software Image, on page 338](#).
You can only mark a SMU as golden if you previously marked the corresponding software image as golden.
- Note** Cisco DNA Center does not allow you to import software images for the FTD devices that are managed by FMC. When you add FMC to inventory and it goes to the Managed state, the software images present in FMC are shown in Image Repository and are categorized based on device family.

Assign a Software Image to a Device Family

After importing a software image, you can assign or unassign it to available device families. The imported image can be assigned to multiple devices at any time.

To assign an imported software image to a device family:

- Step 1** Click the menu icon () and choose **Design > Image Repository**.
- Step 2** Click **Imported Images**.
- Step 3** Click **Assign** in the corresponding image name row.
- Step 4** In the **Assign Device Family** window, choose the **Device Series from Cisco.com** or **All Device Series** and click **Assign** link to which you want to map the image.
Note: If cisco.com credentials are not set, specify the credentials in **System > Settings > Cisco.com Credentials**.
- Step 5** Select appropriate site from the Global hierarchy and click **Assign** and then click **Save**.
- Step 6** To unassign an image, choose a site from the Global hierarchy and click **Unassign** link in the **Action** column.
The software image is assigned to the device family and the number of devices using that image are shown in the **Device(s)** column. After assigning the image, you can mark it as a golden image. See [Specify a Golden Software Image](#).
If the device family is marked as a golden image, you cannot delete that image from the device family.

Note For PnP devices, you can import a software image and assign it to a device family even before the device is available. You can also mark the image as a golden image. When the device is made available in the inventory, the image that is assigned to the device family is automatically assigned to the newly added devices of that device family.

When the image is imported and Cisco DNA Center has cisco.com credentials added, Cisco DNA Center provides the list of device families that are applicable for the image. You can select the required device family from the list.

When the image is not available in cisco.com or when credentials are not added in Cisco DNA Center, you must design the right device family for the image.

Upload Software Images for Devices in Install Mode

The Image Repository page might show a software image as being in Install Mode. When a device is in Install Mode, Cisco DNA Center is unable to upload its software image directly from the device. When a device is in Install Mode, you must first manually upload the software image to the Cisco DNA Center repository before marking the image as golden, as shown in the following steps.

-
- Step 1** Click the menu icon (☰) and choose **Design > Image Repository**.
 - Step 2** In the **Image Name** column, find the software image of the device that is running in **Install Mode**.
 - Step 3** Click **Import** to upload the binary software image file for the image that is in Install Mode.
 - Step 4** Click **Choose File** to navigate to a software image stored locally or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.
 - Step 5** Click **Import**.
A window displays the progress of the import.
 - Step 6** Click **Show Tasks** and verify that the software image you imported is green, indicating it has been successfully imported and added to the Cisco DNA Center repository.
 - Step 7** Click **Refresh**.
The Image Repository window refreshes. Cisco DNA Center displays the software image, and the Golden Image and Device Role columns are no longer dimmed.
-


About Golden Software Images

Cisco DNA Center allows you to designate software images and SMUs as *golden*. A golden software image or SMU is a validated image that meets the compliance requirements for the particular device type. Designating a software image or SMU as golden saves you time by eliminating the need to make repetitive configuration changes and ensures consistency across your devices. You can designate an image and a corresponding SMU as golden to create a standardized image. You can also specify a golden image for a specific device role. For example, if you have an image for the Cisco 4431 Integrated Service Routers device family, you can further specify a golden image for those Cisco 4431 devices that have the Access role only.

You cannot mark a SMU as golden unless the image to which it corresponds is also marked golden.

Specify a Golden Software Image

You can specify a golden software image for a device family or for a particular device role. The device role is used for identifying and grouping devices according to their responsibilities and placement within the network.

Step 1 Click the menu icon () and choose **Design > Image Repository**.

The software images are displayed according to device type.

Step 2 From the **Family** column, select a device family for which you want to specify a golden image.

Step 3 From the **Image Name** column, select the software image that you want to specify as golden.

Step 4 If the software image that you specify as golden is already uploaded into the Cisco DNA Center repository, click the star icon in the **Golden Image** column.

The software image is marked as golden.

Step 5 If the software image that you specify as golden is not already uploaded into the Cisco DNA Center repository, click the download icon in the **Golden Image** column.

This process might take some time.

Note Importing software images from devices is not allowed.

Step 6 From the **Download Image** dialog box, do one of the following:

- Keep the **Mark the image as golden after download** check box checked by default and click **Download**. The software image is downloaded and marked as golden.

Note If Cisco.com credentials are not set, you are prompted to specify them.

The in-progress software image download is shown in the **Device Role** column.

If the software image is downloaded and successfully marked as golden, the color of the star icon turns gold. If the software image download fails, the color of the star icon turns red and a **Please Retry** status is displayed.

- Uncheck the **Mark the image as golden after download** check box and click **Download**. The software image is downloaded to the repository but is not marked as golden.

Step 7 In the **Device Role** column, select a device role for which you want to specify a golden software image. Even if you have devices from the same device family, you can specify a different golden software image for each device role. Note that you can select a device role for physical images only, not virtual images.

Configure an Image Distribution Server

An image distribution server helps in the storage and distribution of software images. You can configure up to three external image distribution servers to distribute software images. You can also set up one or more protocols for the newly added image distribution servers.

For information about the supported servers, see the Server Requirements for Automation Data Backup section in the “Backup Server Requirements” topic in the *Cisco DNA Center Administrator Guide*.

Step 1 Click the menu icon (☰) and choose **System > Settings > Device Settings > Image Distribution Servers**.

Step 2 In the **Image Distribution Servers** window, click **Servers**.

The table displays details about the host, username, SFTP, SCP, and connectivity of image distribution servers.

Step 3 Click **Add** to add a new image distribution server.

The **Add a New Image Distribution Server** slide-in pane is displayed.

Step 4 Configure the following image distribution server settings:

- **Host:** Enter the hostname or IP address of the image distribution server.

- **Root Location:** Enter the working root directory for file transfers.

Note For Cisco AireOS Wireless Controllers, image distribution fails if the configured path is longer than 16 characters.

- **Username:** Enter a username to log in to the image distribution server. The username must have read/write privileges in the working root directory of the server.

- **Password:** Enter a password to log in to the image distribution server.

- **Port Number:** Enter the port number on which the image distribution server is running.

Step 5 Click **Save**.

Step 6 Because some legacy wireless controller software versions support only weak ciphers (such as SHA1-based ciphers) for SFTP, Cisco DNA Center should enable SFTP compatibility mode for SFTP connections from wireless controllers for software image management and wireless assurance. You can temporarily enable support for weak ciphers on the Cisco DNA Center SFTP server for up to 90 days. To allow weak ciphers:

a) Hover over the **i** icon next to the IP address of the SFTP server and click **Click here**.

b) In the **Compatibility Mode** slide-in pane, check the **Compatibility Mode** check box and enter a duration (from 1 minute to 90 days).

c) Click **Save**.

Step 7 (Optional) To edit the settings, click the **Edit** icon next to the corresponding image distribution server, make the required changes, and click **Save**.

Step 8 (Optional) To delete an image distribution server, click the **Delete** icon next to the corresponding image distribution server and click **Delete**.

Change the Protocol Order of an Image Distribution Server

You can change the protocol order of an image distribution server. Protocol order helps in performing verification checks on the image distribution servers. By default, the software images are distributed using the first protocol in the protocol order.

Step 1 Click the menu icon (☰) and choose **System > Settings > Device Settings > Image Distribution Servers**.

Step 2 In the **Image Distribution Servers** window, click **Preferences**.

The default protocol order is shown.

Step 3 Click the **On/Off** toggle button to enable or disable a protocol.

Note The HTTPS or SCP protocol must be enabled for image distribution. The SFTP protocol must be enabled for all protocol orders.

If the HTTPS protocol is disabled or image distribution has failed while using the HTTPS protocol, the software image will be distributed using the SCP protocol.

Step 4 Drag and drop the protocols to change the protocol order.

Step 5 Click **Save**.

Add Image Distribution Servers to Sites

You can associate SFTP servers located in different geographical regions to sites, buildings, and floors. All the devices under the network hierarchy use the associated image distribution server during a network upgrade.

Before you begin

You must configure an image distribution server. See [Configure an Image Distribution Server, on page 339](#).

Step 1 Click the menu icon (☰) and choose **Design > Network Settings**.

Step 2 In the left pane, choose the desired site to which you want to associate the image distribution server.

Step 3 Click **Add Servers**.

Step 4 In the **Add Servers** window, check the **Image Distribution** check box.

Step 5 Click **OK**.

Step 6 Click the **Primary** drop-down list and choose the image distribution server that you want to configure as primary.

Step 7 Click the **Secondary** drop-down list and choose the image distribution server that you want to configure as secondary.

Step 8 Click **Save**.

Provision a Software Image

Cisco DNA Center compares each device software image with the image that you have designated as golden for that specific device type. If there is a difference between the software image and the golden image, Cisco DNA Center specifies that the software image of the device is outdated. If this is the case, you can update the outdated software image.

Before pushing a software image to a device, Cisco DNA Center performs upgrade readiness prechecks on the devices, such as checking the device management status, disk space, and so on. If any prechecks fail, you cannot perform the software image upgrade. You need to correct any issues before you can upgrade the software image on the devices.

If all the prechecks succeed, you can distribute (copy) the new image to the device and activate it (that is, make the new image the running image). The activation of the new image requires a reboot of the device. Because a reboot might interrupt the current network activity, you can schedule the process for a later time.

After the software image is successfully upgraded, Cisco DNA Center performs upgrade postchecks, such as checking the CPU usage, route summary, and so on, to ensure that the state of the network remains unchanged.

Before you begin

- Make sure the device type has a designated golden image. See [Specify a Golden Software Image, on page 338](#).
- If you need to update (distribute and activate) the software image immediately and the **SWIM Events for ITSM (ServiceNow)** bundle is enabled, you need to disable the bundle and its integration workflow (image update schedule approval in ServiceNow). To access the bundle, choose **Platform > Manage > Bundles > SWIM Events for ITSM (ServiceNow)**. Click the **Disable** button in the **SWIM Events for ITSM (ServiceNow)** window. Wait a few seconds before proceeding to update the image, because the process to disable the bundle and workflow takes a few seconds.

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

Step 2 From the **Focus** drop-down list, choose **Software Images**. Select the device whose image you want to upgrade.

Note If the prechecks succeed for a device, the **Outdated** link in the **Software Image** column has a green check mark. If any of the upgrade readiness prechecks fail for a device, the **Outdated** link has a red check mark, and you cannot update the software image for that device. Click the **Outdated** link and correct the errors before proceeding. See [List of Device Upgrade Readiness Prechecks](#).

Step 3 From the **Actions** drop-down list, choose **Software Images > Update Image**.
The **Image Upgrade** window opens.

Step 4 In the **Analyze Selection** step, do the following:

- a) Hover your mouse over the Info icon to view the validation criteria and the CLI commands that are used for validation.
- b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
- c) Click **Next**.

Step 5 In the **Distribute** step, choose whether you want to start the distribution now or schedule it for later.

Note If you associated the external image distribution server with a network hierarchy, the image distribution server distributes the image to all devices under the network hierarchy. See [Add Image Distribution Servers to Sites](#), on page 340.

Step 6 (Optional) To add new custom prechecks and postchecks, click the **add a new check** link, and in the **Add a New Custom Check** window, do the following:

- a) Enter the **Name** for the custom check.
- b) In the **When** drop-down list, choose **pre**, **post**, or both.
- c) In the **Select a Test Device** drop-down list, choose the device you want to check.
- d) Click **Open Command Runner** and enter the CLI commands.
- e) Expand the **Additional Criteria** area.
- f) In the **Operation** drop-down list, choose **Distribution**.
- g) In the **Device Series** drop-down list, choose the series of the device you want to check.
- h) Click **Save**.

Step 7 Click **Next**.

Step 8 In the **Activate** step, choose whether you want to start the activation now or schedule it for later.

Step 9 Check the **Initiate Flash Cleanup after Activation** check box to remove all the previous software images saved on the device.

Note Cisco DNA Center stores only the running software image and removes all the previous software images saved on the device.

Step 10 To choose the validators you want to run for the current workflow, do the following:

- a) Hover your mouse over the Info icon to view the validation criteria and the CLI commands that are used for validation.
- b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.

Step 11 (Optional) To add new custom prechecks and postchecks, click the **add a new check** link, and in the **Add a New Custom Check** window, do the following:

- a) Enter the **Name** for the custom check.
- b) In the **When** drop-down list, choose **pre**, **post**, or both.
- c) In the **Select a Test Device** drop-down list, choose the device you want to check.
- d) Click **Open Command Runner** and enter the CLI commands.
- e) Expand the **Additional Criteria** area.
- f) In the **Operation** drop-down list, choose **Activation**.
- g) In the **Device Series** drop-down list, choose the series of the device you want to check.
- h) Click **Save**.

Step 12 Click **Next**.

Step 13 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 14 To proceed, click **Submit**.

Step 15 (Optional) To check the status of the update, from the **Actions** drop-down list, choose **Software Images > Image Update Status**.

Import the ISSU Compatibility Matrix

In-Service Software Upgrade (ISSU) is a process that upgrades an image on a device with no or minimal service interruption. ISSU is supported only within or between long-lived releases, such as 17.3.x to 17.3.y or 17.3.x to 17.6.y. For an example of the Cisco IOS XE ISSU compatibility matrix for Catalyst Switches, see <https://software.cisco.com/download/home/286315874/type/286326638/release/17.6.2>. You can download and import the ISSU compatibility matrix that corresponds to the target release in Cisco DNA Center to upgrade devices with ISSU.

-
- Step 1** Click the menu icon (☰) and choose **Design > Image Repository**.
 - Step 2** Click **Import Images**.
 - Step 3** In the **Import Image/Add-on** slide-in pane, click the **Select ISSU compatibility matrix** radio button and click **Choose a file** to navigate to an ISSU compatibility matrix file stored locally.
 - Step 4** Click **Import**.
 - Step 5** Click **Show Tasks** to view the ISSU compatibility matrix file import status.
-

Upgrade a Software Image with ISSU

Upgrading devices using the In-Service Software Upgrade (ISSU) eliminates the need to reboot and reduces service interruption.

Before you begin

- Before you upgrade a device using the ISSU, you must import the ISSU compatibility matrix file. See [Import the ISSU Compatibility Matrix, on page 343](#).
- If you need to update the image immediately, the bundle and its integration workflow (image update schedule approval in ServiceNow) must first be disabled. To access the bundle, choose **Platform > Manage > Bundles > SWIM Events for ITSM (ServiceNow)**. Click the **Disable** button in the **SWIM Events for ITSM (ServiceNow)** window. Wait several seconds before updating the image, because the process to disable the bundle and workflow takes several seconds.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
 - Step 2** From the **Focus** drop-down list, choose **Software Images** and choose the device whose image you want to upgrade.
 - Step 3** From the **Actions** drop-down list, choose **Software Images > Update Image**.
The **Image Upgrade** window appears.
 - Step 4** In the **Analyze Selection** window, enable the ISSU upgrade:
 - a) Choose the device that you want to upgrade with ISSU.

Note The **To Image** column shows the ISSU validation status.

- **ISSU shown in amber:** ISSU validation failed because the selected image is not ISSU compatible.
- **ISSU shown in gray:** ISSU validation succeeded and the device supports ISSU.

- b) From the **ISSU** drop-down list, choose **Enable ISSU Upgrade**.
- c) Click **Next**.

Step 5

From the **Distribute** window, choose whether you want to start the image distribution **Now** or schedule it for later. To choose the validators you want to run for the current workflow and add new custom checks, do the following:

- a) Hover your cursor over the Info icon to view the validation criteria and the CLI commands that are used for validation.
- b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.
- c) (Optional) To add new custom prechecks and postchecks, do the following:
 1. Click **add a new check** to launch the **Add a New Custom Check** window.
 2. Enter the **Name** for the custom check.
 3. Click the **When** drop-down list and choose **pre**, **post**, or **both**.
 4. From the **Select a Test Device** drop-down list, choose a device for which you want to run the custom checks.
 5. Click **Open Command Runner** and enter the CLI commands.
 6. Expand the **Additional Criteria** area.
 7. Click the **Operation** drop-down arrow and choose **Distribution**.
 8. Click the **Device Series** drop-down arrow and choose the device series for which you want to run the custom checks.
 9. Click **Save**.
 10. If you want to edit a custom check, click the corresponding More icon, choose **Edit**, make the required changes, and click **Save**.
 11. If you want to delete a custom check, click the corresponding More icon, choose **Delete**, and in the **Confirm Delete** message, click **Delete**.

- Note**
- If associated with a network hierarchy, the external image distribution server distributes the image to all devices in the network hierarchy. See [Add Image Distribution Servers to Sites, on page 340](#).
 - If the **SWIM Events for ITSM (ServiceNow)** bundle is enabled, you need to update the image (distribute and activate) at a later time.

Step 6 Click **Next**.

Step 7 In the **Activate** window, choose whether you want to start the activation **Now** or schedule it for later.

Step 8 Check the **Initiate Flash Cleanup after Activation** check box to remove all the previous software images saved on the device.

- Note** Cisco DNA Center stores only the running software image and removes all the previous software images saved on the device.

To choose the validators you want to run for the current workflow and add new custom checks, do the following:

- a) Hover your cursor over the Info icon to view the validation criteria and the CLI commands that are used for validation.
- b) Click the toggle button to uncheck the validators that you do not want to run for the current workflow.

- c) (Optional) To add new custom prechecks and postchecks, do the following:
1. Click **add a new check** link to launch the **Add a New Custom Check** window.
 2. Enter the **Name** for the custom check.
 3. Click the **When** drop-down list and choose **pre**, **post**, or **both** as required.
 4. Click **Select a Test Device** drop-down list and choose a device for which you want to run these custom checks.
 5. Click **Open Command Runner** and enter the CLI commands.
 6. Expand the **Additional Criteria** area.
 7. Click the **Operation** drop-down list and choose **Activation**.
 8. Click the **Device Series** drop-down list and choose the device series for which you want to run these custom checks.
 9. Click **Save**.
 10. If you want to edit a custom check, click the corresponding More icon, choose **Edit**, make the required changes, and click **Save**.
 11. If you want to delete a custom check, click the corresponding More icon, choose **Delete**, and click **Delete** in the **Confirm Delete** message.

Step 9 Click **Next**.

Step 10 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 11 From the **Actions** drop-down list, choose **Software Images** > **Image Update Status** and check the status of the update.

List of Device Upgrade Readiness Prechecks

Precheck	Description
File transfer check	Checks if the device is reachable through HTTPS and SCP. The default order of protocols is HTTPS first and then SCP.
NTP clock check	Compares device time and Cisco DNA Center time to ensure successful Cisco DNA Center certificate installation.
Flash check	Verifies if there is enough disk space for the update. If there is not enough disk space, a warning or error message is returned. For information about the supported devices for Auto Flash cleanup and how files are deleted, see Auto Flash Cleanup .
Config register check	Verifies the config registry value.
Crypto RSA check	Checks whether an RSA certificate is installed.
Crypto TLS check	Checks whether the device supports TLS 1.2.
IP Domain name check	Checks whether the domain name is configured.

Precheck	Description
Startup config check	Checks whether the startup configuration exists for the device.
NFVIS Flash check	Checks whether the golden image is ready to be upgraded in the NFVIS device.
Service Entitlement check	Checks whether the device has a valid license.

View Image Update Status

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 2** From the **Focus** drop-down list, choose **Software Images**.
- Step 3** From the **Actions** drop-down list, choose **Software Images > Image Update Status**.
By default, the **Image Update Status** window shows all the image update tasks.
- Step 4** To filter the tasks based on the update status, click **In Progress**, **Success**, or **Failure**.
- Step 5** In the left pane, click **Task Names** or **Image Versions** to filter the tasks based on operations or image versions.
The **Status** column shows the current status of the tasks. For in-progress tasks, a progress bar shows the progress of the image update.
- Step 6** Click the device name to view detailed information about a task. For more information, see [View Image Update Workflow, on page 346](#).
- Step 7** Click **Upcoming Tasks** to view the tasks that are scheduled for a later time.
The **Upcoming Tasks** slide-in pane appears.
- Step 8** Click the number of devices in the **Devices Scheduled** column to view the devices for which the image update task is scheduled.
- Step 9** Select the devices for which tasks failed by checking check boxes and click **Retry** to retry the image update.
The **Image Upgrade** window appears. From this window, you can schedule an image update task immediately or later. For more information, see [Provision a Software Image, on page 341](#).
-

View Image Update Workflow

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 2** From the **Focus** drop-down list, choose **Software Images**.
- Step 3** From the **Actions** drop-down list, choose **Software Images > Image Update Status**.
- Step 4** In the **Image Update Status** window, click the name of a device to view detailed information about the image upgrade.
- Step 5** Click the **Operations** tab.
The slide-in pane shows the status of each task that is associated with the **Distribution** and **Activation** operations and the time taken to complete each operation.

Step 6 Expand **Distribution** to view the status of the following tasks that are associated with the **Distribution** operation and the time taken to complete each task.

- **Verify Image Availability** (only for legacy devices): Verifies the software image in **Image Repository**
- **Image Integrity Verification (KGV)**: Compares the software and hardware platform checksum value of the software image with the checksum value identified for the platform in the Known Good Values (KGV).
- **Pre Distribution Operation**: Performs all the prechecks chosen for software image distribution.
- **Distribution**: Distributes the software image through the primary external image distribution server.
If the software image distribution fails through primary external image distribution server, the software image is distributed through secondary image distribution server. If the distribution fails through both the external servers, the software image is distributed through the internal Cisco DNA Center server.
- **Post Distribution Operation**: Performs all the post checks chosen for software image distribution.
- **Image Checksum Verification On Device**: Verifies the checksum value of the software image on the device.
- **Unpack Image** (only for Polaris): Executes the `install-add` command from the CLI. Unpack image is performed only when the image is in install mode.
- **AP Pre-Image Download** (only for access points): Shows details about the distribution process of all the access points associated with the device.

Step 7 Expand **Activation** to view the status of the following tasks that are associated with the **Activation** operation and the time taken to complete each task.

- **Pre Activation Operation**: Performs all the prechecks chosen for software image activation.
- **Image Activation**: Executes the `install-activate` command in CLI. This shows detailed information about the image activation process.
Note For Cisco Catalyst 9000 Series stack switches, the `Validate Stack` prechecks verifies the state of all the stack members in a switch. If a stack member is not running the golden image, run the `auto-upgrade` command.
- **Staggered AP Upgrade** (only for access points): Shows details about activation process of all the access points associated with the device.
- **Install Commit** (only for Polaris): Executes the `install-commit` command from the CLI.
- **Remove Inactive Images**: Removes all the previous software images saved on the device and stores only the running image.
- **Collect Running Image Details**: Collects the running image details.
- **Verify Image Activation**: Verifies whether the software image is upgraded properly.
- **Post Activation Operation**: Performs all the postchecks chosen for software image activation.

Note

- For Cisco Catalyst 9800 Embedded Wireless Controller devices and Cisco Catalyst 9000 Series Switches running on Cisco IOS-XE software, the software image is upgraded in three steps (by executing three commands)—**install-add** (Unpack Images step in Distribution), **install-activate** (Image Activation step in Activation), and **install-commit** (Install Commit step in Activation).
- If the device is in Inactive state, run the `install-add` command from the CLI. Subsequently run the `install-activate` and `install-commit` commands. If the device is in Uncommitted state, run the `install-commit` command directly.
- Run the `install-activate` and `install-commit` commands sequentially in separate milestones during activation, so that you can abort, roll back, or commit the update.

Step 8 Click the **Tasks** tab.

Step 9 The **Tasks** tab shows the status and details of prechecks and postchecks that are associated with the task. Click the number of differences in the **Differences** column, corresponding to each script, to view the differences between prechecks and postcheck.

Auto Flash Cleanup

During the device upgrade readiness precheck, the flash check verifies whether there is enough space on the device to copy the new image. If there is insufficient space:

- **For devices that support auto flash cleanup**, the flash check fails with a warning message. For these devices, the auto cleanup is attempted during the image distribution process to create the sufficient space. As a part of the auto flash cleanup, Cisco DNA Center identifies unused `.bin`, `.pkg`, and `.conf` files and deletes them iteratively until enough free space is created on the device. Image distribution is attempted after the flash cleanup. You can view these deleted files in **System > Audit Logs**.



Note Auto flash cleanup is supported on all devices except Nexus switches and wireless controllers.

- **For devices that do not support auto flash cleanup**, the flash check fails with an error message. You can delete files from the device flash to create space before starting the image upgrade.



CHAPTER 14

Compliance Audit for Network Devices

- [Compliance Overview, on page 349](#)
- [Types of Compliance, on page 350](#)
- [View Compliance Summary, on page 353](#)
- [Manual Compliance Run, on page 354](#)
- [Generate a Compliance Audit Report for Network Devices, on page 354](#)
- [Acknowledge Compliance Violations, on page 355](#)
- [Synchronize Startup and Running Configurations of a Device, on page 356](#)
- [Fix Compliance Violations, on page 356](#)
- [Compliance Behavior After Device Upgrade, on page 357](#)
- [Limitations in CLI Template Compliance, on page 358](#)

Compliance Overview

Compliance helps in identifying any intent deviation or *out-of-band* changes in the network that may be injected or reconfigured without affecting the original content.

A network administrator can conveniently identify devices in Cisco DNA Center that do not meet compliance requirements for the different aspects of compliance, such as software images, PSIRT, network profiles, and so on.

Compliance checks can be automated or performed on demand.

- **Automated compliance check:** Uses the latest data collected from devices in Cisco DNA Center. This compliance check listens to the traps and notifications from various services, such as inventory and SWIM, to assess data.
- **Manual compliance check:** Lets you manually trigger the compliance in Cisco DNA Center.
- **Scheduled compliance check:** A scheduled compliance job runs every day at 11:00 pm and triggers the compliance check for devices on which the compliance check was not run in the past seven days.

Types of Compliance

Compliance Type	Compliance Check	Compliance Status
Startup versus Running Configuration	This compliance check helps in identifying whether the startup and running configurations of a device are in sync. If the startup and running configurations of a device are out of sync, compliance is triggered and a detailed report of the out-of-band changes is displayed. The compliance for startup vs. running configurations is triggered within 5 minutes of any out-of-band changes.	<ul style="list-style-type: none"> • Noncompliant: The startup and running configurations are not the same. In the detailed view, the system shows different startup vs. running between or running vs. previous running. • Compliant: The startup and running configurations are the same. • NA (Not Applicable): The device, such as AireOS, is not supported for this compliance type.
Software Image	This compliance check helps a network administrator to see if the tagged golden image in Cisco DNA Center is running on the device. It shows the difference between the golden image and the running image for a device. When there is a change in the software image, the compliance check is triggered immediately without any delay.	<ul style="list-style-type: none"> • Noncompliant: The device is not running the tagged golden image of the device family. • Compliant: The device is running the tagged golden image of the device family. • NA (Not Applicable): The golden image is not available for the selected device family.
	For Cisco Switch Stacks: Cisco DNA Center allows the network administrator to check if the tagged golden image is running on master switch and members of switch stacks.	<ul style="list-style-type: none"> • Noncompliant: The tagged golden image is not running on master switch and member switches. • Compliant: The tagged golden image is running on master switch and member switches. • NA (Not Applicable): The golden image is not available for the selected device.
Critical Security (PSIRT)	This compliance check enables a network administrator to check whether the network devices are running without critical security vulnerabilities.	<ul style="list-style-type: none"> • Noncompliant: The device has critical advisories. A detailed report displays various other information. • Compliant: There are no critical vulnerabilities in the device. • NA (Not Applicable): The security advisory scan has not been done by the network administrator in Cisco DNA Center, or the device is not supported.

Compliance Type	Compliance Check	Compliance Status
Network Profile	<p>Cisco DNA Center allows you to define its intent configuration using network profiles and push the intent to the device. If any violations are found at any time due to <i>out-of-band</i> or any other changes, this check identifies, assesses, and flags it off. The violations are shown to the user under Network Profiles in the compliance summary window.</p> <p>Note Network profile compliance is applicable for routers, switches and wireless controllers.</p>	<ul style="list-style-type: none"> • Noncompliant: The device is not running the intent configuration of the profile. • Compliant: While applying a network profile to the device, the device configurations that are pushed through Cisco DNA Center are actively running on the device. • Error: The compliance could not compute the status because of an underlying error. For details, see the error log.
Fabric (SDA) This feature is in beta.	Fabric compliance helps to identify fabric intent violations, such as any out-of-band changes for fabric-related configurations.	<ul style="list-style-type: none"> • Noncompliant: The device is not running the intent configuration. • Compliant: The device is running the intent configuration.
Application Visibility	<p>Cisco DNA Center allows you to create an application visibility intent and provision it to a device through CBAR and NBAR. If there is an intent violation on the device, this check identifies, assesses, and shows the violation as compliant or noncompliant under the Application Visibility window.</p> <p>The automatic compliance checks are scheduled to run after 5 hours of receiving traps.</p>	<ul style="list-style-type: none"> • Noncompliant: The CBAR/NBAR configuration is not running on the device. • Compliant: The intent configuration of CBAR/NBAR is running on the device.
Model Config	This compliance check enables the network administrator to check any mismatch from the designed intent of Model Config. The mismatch is shown under Network Profile in the Compliance Summary window.	<ul style="list-style-type: none"> • Noncompliant: There is a mismatch in the actual and intended value of attributes in Model Config. • Compliant: The attributes in Model Config match the intended value.

Compliance Type	Compliance Check	Compliance Status
CLI Template	<p>Cisco DNA Center allows the network administrator to compare the CLI template with the running configuration of the device. The mismatch in the configuration is flagged. The mismatch is shown under Network Profile in the Compliance Summary window.</p> <p>The running configuration for CLI template compliance is taken from the latest archive that is available for the device. Event-based archive takes at least 5 minutes to update after traps are received. For accurate results, we recommend that you wait for at least 5 minutes before running compliance manually after a configuration change.</p> <p>Note There are some limitations in CLI template compliance. See Limitations in CLI Template Compliance, on page 358.</p>	<ul style="list-style-type: none"> • Noncompliant: There is mismatch between the CLI template and the running configuration of the device. • Compliant: There is no mismatch between the CLI template and the running configuration of the device.
EoX - End of Life	<p>Cisco DNA Center allows you to check compliance status for hardware, software, and module of EoX devices. You can check the EoX compliance status from the Compliance Summary > EoX - End of Life tile.</p> <p>You can also view the EoX status of devices from the Inventory window, under the EoX Status column.</p>	<ul style="list-style-type: none"> • Compliant: The device is compliant if enough time remains until the last date of support. • Noncompliant: The device is noncompliant if the last date of support has ended. • Compliant with Warning: The device is compliant with warning if the last date of support is nearing.
Network Settings	<p>Cisco DNA Center allows you to define its intent configuration settings using network settings and push the intent to the device. If any violations are found at any time due to out-of-band or any other changes, compliance check identifies, assesses, and flags it off.</p> <p>You can view the violations under Network settings in the Compliance Summary window.</p> <p>Note Post UI upgrade, compliance for network settings will get triggered after six hours.</p>	<ul style="list-style-type: none"> • Compliant: The intent configuration that are pushed are actively running on the device. • Noncompliant: The device is not running the intent configuration. • NA (Not Applicable): The device is not configured with network settings, or the device is not assigned to the site.

Compliance Type	Compliance Check	Compliance Status
Cisco Umbrella	<p>Cisco DNA Center allows you to identify the deviation from the intent Cisco Umbrella configuration pushed to the device by Cisco DNA Center. If any violations are found compliance check identifies, assesses and flags it off.</p> <p>You can view the violations under Workflow in the Compliance Summary window.</p> <p>Note Cisco Umbrella compliance check is applicable for Switches or Cisco Embedded Wireless Controllers. Ensure the device provisioning is completed.</p> <p>Also, Cisco Umbrella must be provisioned on the devices. For more information, see Provision Cisco Umbrella on Network Devices, on page 546.</p>	<ul style="list-style-type: none"> • Compliant: The intent configuration that are pushed are actively running on the device. • Noncompliant: Device is not running the intent configuration. • NA (Not Applicable): Cisco Umbrella is not configured for the device.

View Compliance Summary

The inventory page shows an aggregated status of compliance for each device.

Step 1 Click the menu icon (☰) and choose **Provision > Inventory**.

The compliance column shows the aggregated compliance status of each device.

Step 2 Click the compliance status to launch the compliance summary window, which shows the following compliance checks applicable for the selected device:

- Startup versus Running Configuration
- Software Image
- Critical Security Vulnerability
- Network Profile
- Network Settings
- Fabric
- Application Visibility
- EoX - End of Life
- Cisco Umbrella

Note Network Settings, Network Profile, Fabric, and Application Visibility are optional and are displayed only if the device is provisioned with the required data.

Manual Compliance Run

You can trigger a compliance check manually in Cisco DNA Center.

Step 1 Click the menu icon () and choose **Provision > Inventory**.

Step 2 For a bulk compliance check, do the following:

- a) Choose all the applicable devices.
- b) From the **Actions** drop-down list, choose **Compliance > Run Compliance**.

Step 3 For a per-device compliance check, do the following:

- a) Choose the devices for which you want to run the compliance check.
- b) From the **Actions** drop-down list, choose **Compliance > Run Compliance**.
- c) Alternatively, click the compliance column (if available) and then click **Run Compliance**.

Step 4 To view the latest compliance status of a device, do the following:

- a) Choose the device and inventory. See [Resynchronize Device Information, on page 102](#).
- b) From the **Actions** drop-down list, choose **Compliance > Run Compliance**.

Note

- A compliance run cannot be triggered for unreachable or unsupported devices.
- If compliance is not run manually for a device, the compliance check is automatically scheduled to run after a certain period of time, which depends on the type of compliance.
- CLI Template Compliance compares the realized templates against the running configuration of the device. The running configuration is taken from the latest archive that is available for the device.
Event-based archive takes at least 5 minutes to update after traps are received. For accurate results, we recommend that you wait for at least 5 minutes before running compliance manually after a configuration change.

Generate a Compliance Audit Report for Network Devices

Cisco DNA Center allows you to retrieve a consolidated Compliance Audit Report that shows the compliance status of individual network devices. With this report, you can get complete visibility of your network.

For more information, see "Run a Compliance Report" in the [Cisco DNA Center Platform User Guide](#).

Acknowledge Compliance Violations

Cisco DNA Center lets you acknowledge less-important compliance violations of the device and opt-out the violations from the compliance status calculation. If required, you can also choose to opt-in the violation for the compliance status calculation.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** Click the device name to open a dialog box that provides high-level information for that device. Click **View Device Details** link in the dialog box.
The device details window is displayed.
- Step 3** In the left pane, choose **Compliance > Summary**.
- Step 4** In the **Compliance Summary** window, click the compliance tile for which you want to acknowledge the violations.
You can view the following information under **Open Violations** and **Acknowledged Violations** table:
- Model Name
 - Attribute
 - Status: This column shows one of the following status:
 - **Added**: The attribute is added in the device.
 - **Changed**: The intent value does not match the device value.
 - **Removed**: The intent is removed from the device.
 - Intended Value: Shows the intended value as configured by Cisco DNA Center.
 - Actual Value: Shows the value currently configured on the device.
 - Action: Shows **Acknowledge** link for open violations and **Move to Open Violations** link for acknowledged violations.
- Do the following to opt-out the violation from the compliance status calculation:
- a) Click the **Open Violations** tab.
 - b) Choose the violation and click **Acknowledge** in the **Actions** column.
 - c) To acknowledge the violations in bulk, check the check box at the top of the table, or choose multiple violations and click **Acknowledge**.
 - d) In the confirmation window, click **Confirm**.
The violation is moved to the **Acknowledged Violations** tab.
- Do the following to opt-in the violation for the compliance status calculation:
- a) Click the **Acknowledged Violations** tab.
 - b) Choose the violation and click **Move to Open Violations** in the **Actions** column.
 - c) To move the violations in bulk, check the check box at the top of the table, or choose multiple violations and click **Move to Open Violations**.
 - d) In the confirmation window, click **Confirm**.
The violation is moved to **Open Violations** tab.
- Step 5** To see a list of attributes that you opted out from the Compliance status calculation, click the **View Preference for Acknowledged Violations** link in **Compliance Summary** window.

- Step 6** In the **Acknowledge Violation Preferences** slide-in pane, do the following to opt-in the attribute for the compliance status calculation:
- Choose the attribute and click **Unlist** in the **Actions** column.
 - For bulk selection, check the check box at the top of the table, or choose multiple violations and click **Unlist**.
- The **Models** tab shows attributes that are acknowledged for Model Config, Routing, Wireless, Application Visibility, or Fabric. Acknowledged templates are shown under the **Templates** tab.
- Note**
- In **Acknowledge Violation Preferences** window, a model with an empty (-) attribute means that the entire model, including its child attributes, are acknowledged.
 - When a violation with the status, **Added** or **Removed** is acknowledged, Cisco DNA Center automatically acknowledges similar attributes and their child attributes.
 - An acknowledged child attribute cannot be moved to open violations when a similar violation with the status, **Added** or **Removed** is overriding.

Synchronize Startup and Running Configurations of a Device

When there is a mismatch in the startup and running configurations of a device, you can do a remediation synchronization to match the configurations.

- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** For a bulk remediation, do the following:
- Choose all the applicable devices.
 - From the **Actions** drop-down list, choose **Compliance > Write Running Config to Startup Config**.
- For a per-device remediation, do the following:
- Choose the devices for which you want to do a remediation synchronization.
 - From the **Actions** drop-down list, choose **Compliance > Write Running Config to Startup Config**.
- Alternatively, click the link under **Compliance** column and then choose **Compliance Summary > Startup vs Running Configuration > Sync Device Config**.
- Step 3** To view the remedial status of the device, do the following:
- Click the menu icon (☰) and choose **Provision > Inventory**.
 - From the **Actions** drop-down list, choose **Compliance > Check Startup Config Write Status**.

Fix Compliance Violations

Cisco DNA Center allows you to maintain a compliant network by providing an automated fix for device compliance violations. Any deviation from the intent in the device that is identified in the Cisco DNA Center compliance check is fixed with this procedure.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** Click the device name to open a dialog box that provides high-level information for that device. Click **View Device Details** in the dialog box.
The device details window is displayed.
- Step 3** In the left pane, click **Compliance > Summary**.
The **Compliance Summary** window is displayed.
- Step 4** At the top of the window, click **Fix All Configuration Compliance Issues**.
The **Fix Configuration Compliance Issues** slide-in pane is displayed.
- Note** The link for fixing compliance violations is visible only if the supported category has violations. Otherwise, the link is not shown.
- Step 5** In the **Summary of Issues to be Fixed** area, review the violations for the devices. The **Issues Identified** column lists the aggregated count of open and acknowledged violations.
In the **Schedule the Fix** area, do the following:
- If required, modify the default name in the **Task Name** field.
 - Do one of the following:
 - Click **Now** to fix the violation immediately, and click **Apply**.
 - Click **Later** to schedule the fix for a later time, define the date and time, and click **Apply**.
 - Click **Generate Preview** to generate the preview of the remediation, and click **Apply**.
- The **Activities > Work Items** preview link is displayed at the top of the **Compliance Summary** window.
- Step 6** Click the preview link to review the remediation. Click **Deploy** to fix the violation on the selected device.
- Note**
- Routing, Wireless Controller HA Remediation, Software Image, Security Advisories, and Workflow-related compliance issues are not addressed in this fix. You can address these separately by following the actions in their respective sections.
 - CLI template compliance has some limitations, because of which some CLI templates remain noncompliant. For more information, see [Limitations in CLI Template Compliance, on page 358](#).

Compliance Behavior After Device Upgrade

- A compliance check for all applicable devices (devices for which compliance never ran in the system) is triggered after successful device upgrade.
- Compliance calculates and shows the status of the devices in the inventory, except the Startup vs Running type.
- After upgrade, the Startup vs Running tile shows as NA with the text "Configuration data is not available."

- After a day of successful upgrade, a one-time scheduler runs and makes configuration data available for devices. The Startup vs Running tile starts showing the correct status (Compliant/Noncompliant) and detailed data.
- If any traps are received, the config archive service collects configuration data and the compliance check runs again.



Note In the upgrade setup, ignore any compliance mismatch for the **Flex Profile** interface. For the interface name, **1** maps to **management**.

Limitations in CLI Template Compliance

Cisco DNA Center allows you to compare a CLI template with the running configuration of the device, so as to identify any mismatch from the intent. Note the following comparator engine limitations:

- The CLI Template comparator supports use of uppercase letters for variables and values.
- Avoid using uppercase letters for command keywords.
- The CLI Template comparator supports use of aliases.
- Avoid using abbreviated or shorthand commands, which are flagged as noncompliant.
- If a command is missing and it is at the section level, the section-level commands succeeding the missing command are also flagged. To avoid this problem, use indentation.

For example, the following CLI Template comparator output shows commands without indentation:

Realized Template	Running Configuration	Output
<pre>#interface Vlan111 #description SVI interface kan-111 #ip address 111.2.3.4 255.255.255.0 #ip helper-address 7.7.7.8 #no mop enabled #no mop sysid #!</pre>	<pre>#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!</pre>	<p>The following commands are marked as missing:</p> <pre># ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid</pre>

The following CLI Template comparator output shows commands with indentation:

Realized Template	Running Configuration	Output
<pre>#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!</pre>	<pre>#interface Vlan111 # description SVI interface kan-111 # ip address 111.2.3.4 255.255.255.0 # ip helper-address 7.7.7.7 # ip helper-address 7.7.7.8 # no mop enabled # no mop sysid #!</pre>	<p>The comparator flags only the missing command:</p> <pre>#ip helper-address 7.7.7.7</pre>

- Interactive and enable mode commands are not compared for compliance. You can use an alternative form of interactive commands by mentioning all the options and values with the commands.

For example, if the template code is as follows, where **#ENABLE** and **#INTERACTIVE** mode command are given together, the commands are not compared.

```
#MODE_ENABLE
#INTERACTIVE
  mkdir <IQ>Create directory<R>xyz
#ENDS_INTERACTIVE
#MODE_END_ENABLE
#end
```

- Avoid using ranges in commands, which are flagged by the comparator. Ranges must be used in expanded form.
- Overriding commands within the same template are flagged. You can avoid mismatch by enclosing the commands within *ignore - compliance* syntax, as shown in the following example.

Realized Template	Running Configuration	Output
<pre>#no banner motd #Welcome to Cisco .: :.# #banner motd #Welcome to Cisco .: :.#</pre>	<pre>#banner motd ^CWelcome to Cisco .: :.^C</pre>	<ul style="list-style-type: none"> • The following command is flagged as missing: <pre>no banner motd #Welcome to Cisco .: :.#</pre> • The following command is also marked as missing, because the running command is already compared with the preceding command. <pre>banner motd #Welcome to Cisco .: :.#</pre>

You can do the following to avoid mismatch:

Realized Template	Running Configuration	Output
<pre>#! @start-ignore-compliance #no banner motd #Welcome to Cisco .: :.# #! @end-ignore-compliance #banner motd #Welcome to Cisco .: :.#</pre>	<pre>#banner motd ^CWelcome to Cisco .: :.^C</pre>	<p>There is no mismatch, because the command enclosed in the syntax is not compared.</p>

- For later releases of Cisco IOS XE, some default commands are shown only when **show run all** command is issued, instead of the **show run** command. Therefore, these commands do not appear in the running configuration and are flagged as noncompliant.
- Password-bearing commands are flagged by the comparator, because they are stored in encrypted form on the device.



Note You can avoid a mismatch for password-bearing commands and some default commands by enclosing the commands in the following syntax:

```
! @start-ignore-compliance  
! @end-ignore-compliance
```

Then, reprovision the template for the changes to appear.

To avoid a mismatch between the CLI template and the running configuration of the device, we recommend that you use commands similar to the running configuration.



CHAPTER 15

Run Diagnostic Commands on Devices

- [Command Runner Overview](#), on page 361
- [Run Diagnostic Commands on Devices](#), on page 361

Command Runner Overview

The Command Runner tool allows you to send diagnostic CLI commands to selected devices. Currently, **show** and other read-only commands are permitted.

Run Diagnostic Commands on Devices

Command Runner lets you run diagnostic CLI commands on selected devices and view the resulting command output. Command Runner supports only a subset of the shortcuts that are available as part of a standalone terminal.

Before you begin

Begin using Command Runner, do the following:

1. Click the menu icon (☰) and choose **System > Software Updates > Installed Apps**.
2. Find the **Command Runner** application and click **Install**.
3. After installation, run a Discovery job to populate Cisco DNA Center with devices. You are presented with a list of devices from which to run diagnostic CLI commands.

-
- Step 1** Click the menu icon (☰) and choose **Tools > Command Runner**.
- Step 2** In the **Search** field of the **Command Runner** window, click the drop-down arrow to search by **Device IP** or **Device Name**.
- Step 3** Choose a device or devices on which to run diagnostic CLI commands.
Device List displays your selection.
- Step 4** (Optional) Select another device to add to the list. You can select up to 20 reachable devices.

Note Although the device list displays everything available in inventory, Command Runner is not supported for wireless access points and Cisco Meraki devices. If you choose an access point device or Cisco Meraki device, a warning message appears, stating that no commands will be executed on them.

Step 5 In the **Select/Enter commands** field, enter a CLI command and click **Add**.

Command Runner supports type ahead. As you begin typing, Command Runner displays the commands available for you to choose. You can also type a new, valid command.

Step 6 Click **Run Command(s)**.

If successful, a `Command(s) executed successfully` message appears.

Step 7 Click the command displayed underneath the device to view the command output.

Note The complete command output is displayed in the **Command Runner** window. Any sensitive information, such as passwords, is masked in the command output.

Step 8 (Optional) Click **Export all CLI Output** to export the command output to a text file that you can save locally.

Step 9 Click **Go Back** to return to the previous window.

Note If necessary, click the **x** next to a device name to remove the device from the device list. Similarly, click the **x** next to a command to remove the command from the list.



PART **V**

Provision Your Network

- [Onboard and Provision Devices with Plug and Play, on page 365](#)
- [Provision Wireless Devices, on page 389](#)
- [Provision a Routing Profile, on page 447](#)
- [Provision Firewall Profiles, on page 451](#)
- [Provision a LAN Underlay, on page 453](#)
- [Provision Fabric Networks, on page 463](#)
- [Provision Services, on page 513](#)



CHAPTER 16

Onboard and Provision Devices with Plug and Play

- [Plug and Play Provisioning Overview](#), on page 365
- [Plug and Play Provisioning Prerequisites](#), on page 367
- [Plug and Play Deployment Guidelines](#), on page 372
- [View Devices](#), on page 372
- [Add or Edit a Device](#), on page 374
- [Add Devices in Bulk](#), on page 375
- [Register or Edit a Virtual Account Profile](#), on page 376
- [Add Devices from a Smart Account](#), on page 377
- [Provision a Device with Plug and Play](#), on page 378
- [Delete a Device](#), on page 387
- [Reset a Device](#), on page 387

Plug and Play Provisioning Overview

Plug and Play provisioning provides a way to automatically and remotely provision and onboard new network devices with minimal network administrator and field personnel involvement.

Using Plug and Play provisioning, you can do the following:

- Provision devices by assigning a site, deploying site settings, installing a device software image, and applying a custom onboarding configuration.
- Plan devices before their installation by entering device information and choosing provisioning operations. When the device comes online, it contacts Cisco DNA Center and Plug and Play provisions and onboards the device automatically.
- Provision unclaimed network devices, which are new devices that appear on the network, without prior planning.
- Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal in a Cisco Smart Account to Plug and Play, so that all the devices appear in Cisco DNA Center.
- Display the detailed onboarding status of network devices.

The following sections describe typical use cases and workflows for Plug and Play provisioning.

Planned Provisioning

An administrator can plan the provisioning of a new site or other group of network devices as follows:

1. We recommend that you define the site within the network hierarchy. See [Network Hierarchy Overview, on page 125](#).
2. Define Onboarding Configuration templates to be applied to devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. In many cases, such templates are not necessary unless you need to customize the Day 0 configuration. See [Create Templates to Automate Device Configuration Changes, on page 291](#).



Note Day 0 templates do not support Interactive commands.

3. Define network profiles for the types of devices you are deploying. See [Network Profiles Overview, on page 275](#).
4. We recommend that you define the device credentials (CLI and SNMPv2c/SNMPv3) for the devices you are deploying. If you are using SNMPv2c, both Read and Write credentials must be provided.



Note Missing credentials will lead to the devices not being able to be added to inventory after they are provisioned.

5. Ensure that software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository. See [Import a Software Image, on page 335](#).
6. Add details about planned devices one at a time or in bulk with a CSV file. See [Add or Edit a Device, on page 374](#) or [Add Devices in Bulk, on page 375](#).
7. Devices boot up and are automatically provisioned.

Unclaimed Provisioning

If a new network device is added to the network before it can be planned, it is labeled as an unclaimed device. An unclaimed device can be added manually by an administrator, or automatically through one of the discovery methods described in [Plug and Play Provisioning Prerequisites, on page 367](#). An administrator can provision the device as follows:

1. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See [View Devices, on page 372](#).
2. Claim the device by assigning a site, image, configuration template, or profile. See [Provision a Device with Plug and Play, on page 378](#). You can also claim the device without assigning a site.



Note Global device credentials are required for devices with no site assigned. Global device credentials at site level are required for devices with sites assigned.

Cisco Smart Account Synchronization and Provisioning

Network devices can be automatically registered through a Cisco Smart Account with the Cisco Plug and Play Connect cloud service. An administrator can synchronize the device inventory from Cisco Plug and Play Connect to Cisco DNA Center Plug and Play, so that all the devices appear in Cisco DNA Center. These devices can then be claimed and provisioned.

1. Register a Smart Account and virtual account with which to synchronize. See [Register or Edit a Virtual Account Profile, on page 376](#).
2. Synchronize the device inventory from the Smart Account. See [Add Devices from a Smart Account, on page 377](#).
3. Find the device on the devices list by filtering on unclaimed devices or searching for it by name. See [View Devices, on page 372](#).
4. Claim the device by assigning a site, image, configuration template, or profile. See [Provision a Device with Plug and Play, on page 378](#).
5. Devices boot up and are automatically provisioned.

Plug and Play Provisioning Prerequisites

Before using Plug and Play provisioning, make sure the required prerequisites are met for all device types. In addition, if you are deploying wireless or sensor devices, make sure those prerequisites are met. Other prerequisites are optional, but if you decide to do them, they must be done before you use Plug and Play to provision devices.

Prerequisites for All Devices

Make sure all device types meet the following prerequisites:

- Make sure devices can automatically discover the Cisco DNA Center controller in one of the following ways:
 - DHCP: See [DHCP Controller Discovery, on page 369](#).
 - DNS: See [DNS Controller Discovery, on page 370](#).
 - Cisco Plug and Play Connect cloud service: See [Plug and Play Connect Controller Discovery, on page 371](#).
- Set the Cisco.com credentials in the main Cisco DNA Center settings by using **System > Settings > Cisco.com Credentials**.
If needed, set the Cisco Smart Account credentials in **System > Settings > Smart Account**.
- Accept the End User License Agreement (EULA) in the main Cisco DNA Center settings by using **System > Settings > Device EULA Acceptance**.
- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in [Network Plug and Play Troubleshooting Guide for Cisco DNA Center](#).

Prerequisites for Wireless or Sensor Devices

In addition to the previous prerequisites, make sure any wireless or sensor devices meet the following requirements:

- For wireless AP devices, ensure that the Cisco Wireless Controller that is managing the wireless APs has been added to the inventory and assigned to the site where the wireless APs are going to be assigned. This requirement is not needed for Mobility Express APs.
- For wireless AP devices, define the wireless radio frequency profiles. See [Create a Wireless Radio Frequency Profile, on page 227](#). This requirement is not needed for Mobility Express APs.
- For Mobility Express APs, define an IP address pool and a management interface. See [Configure IP Address Pools, on page 202](#).
- For ROW APs, we recommend that you create an AP profile with the necessary country code and configure custom site tags. See [Configure Additional Settings for an AP Profile for Cisco IOS XE Devices, on page 259](#) and [Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 285](#).
- Effective with Release 2.3.5.4, you can configure the AP location for PnP onboarding in the **PnP AP Location** window using the **Configure AP Location** check box. This check box is unchecked by default. If necessary, check this check box to configure the site assigned during PnP claim as the AP location during PnP onboarding. For more information, see "Configure AP Location for PnP Onboarding" in the [Cisco DNA Center Administrator Guide](#).
- For sensors, ensure that the sensor is reachable through the Cisco DNA Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Cisco DNA Center; however, to claim the device, it must be reachable from the interface enp9s0 IP address. In the DHCP server, configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with ACSII value "5A1D;B2;K4;I172.16.x.x;J80;", where 172.16.x.x is the virtual IP address of Cisco DNA Center associated with the enp9s0 interface.

Optional Prerequisites

The following prerequisites are optional, but help to automate the Plug and Play provisioning process:

- Define the site within the network hierarchy. See [Network Hierarchy Overview, on page 125](#).
- Define the CLI and SNMP credentials for the devices. See [Global Device Credentials Overview, on page 194](#).



Note You can claim wireless devices using CLI, SNMPv2c, or SNMPv3 credentials. If you use SNMPv2c, provide both Read Only and Read Write credentials.

- Ensure that software images for the devices to be provisioned are uploaded and marked as golden in the Image Repository, if you want to deploy images. See [Import a Software Image, on page 335](#).



Note The image deployment process used by Plug and Play during Day-0 provisioning is not the same as that used when updating a device image later, which is described in [Provision a Software Image, on page 341](#). During Plug and Play provisioning, there are no device prechecks, auto flash cleanup, or post-checks done, as it is expected that devices are in the factory default state.

- Define Onboarding Configuration templates to be applied to devices. Such templates contain basic network configuration commands to onboard a device so that it can be managed on the network. See [Create Templates to Automate Device Configuration Changes, on page 291](#).



Note You can use the `ip http client source-interface` CLI command in the Onboarding Configuration template, which makes Cisco DNA Center use that IP address as the management IP address for the device, especially for the scenario of multiple IPs or VRFs.

- Define network profiles for the devices. See [Network Profiles Overview, on page 275](#).

DHCP Controller Discovery

When a Cisco network device first starts up with no startup configuration, it attempts to discover the Cisco DNA Center controller by using DHCP Option 43.

The prerequisites for the DHCP discovery method are as follows:

- New devices can reach the DHCP server.
- The DHCP server is configured with Option 43 for Cisco Plug and Play. This option informs the network device of the IP address of the Cisco DNA Center controller.

When the DHCP server receives a DHCP discover message from the device, with Option 60 containing the string “ciscopnp”, it responds to the device by returning a response that contains the Option 43 information. The Cisco Plug and Play IOS Agent in the device extracts the Cisco DNA Center controller IP address from the response and uses this address to communicate with the controller.

DHCP Option 43 consists of a string value that is configured as follows on a Cisco router CLI that is acting as a DHCP server:

```
ip dhcp pool pnp_device_pool          <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0     <-- Range of IP addresses assigned to clients
default-router 192.168.1.1           <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80;" <-- Option 43 string
```

The Option 43 string has the following components, delimited by semicolons:

- 5A1N;—Specifies the DHCP suboption for Plug and Play, active operation, version 1, no debug information. It is not necessary to change this part of the string.
- B2;—IP address type:

- B1 = hostname
 - B2 = IPv4 (default)
 - *Lxxx.xxx.xxx.xxx*;—IP address or hostname of the Cisco DNA Center controller (following a capital letter i). In this example, the IP address is 172.19.45.222.
 - *Jxxx*—Port number to use to connect to the Cisco DNA Center controller. In this example, the port number is 80. The default is port 80 for HTTP and port 443 for HTTPS.
 - K4;—Transport protocol to be used between the device and the controller:
 - K4 = HTTP (default)
 - K5 = HTTPS
 - *TrustpoolBundleURL*;—Optional parameter that specifies the external URL of the trustpool bundle if it is to be retrieved from a different location than the default, which is the Cisco DNA Center controller, which gets the bundle from the Cisco InfoSec cloud (<http://www.cisco.com/security/pki/>). For example, to download the bundle from a TFTP server at 10.30.30.10, you would specify the parameter like this: `Tftp://10.30.30.10/ios.p7b`
- If you are using trustpool security and you do not specify the T parameter, the device retrieves the trustpool bundle from the Cisco DNA Center controller.
- *Zxxx.xxx.xxx.xxx*;—IP address of the NTP server. This parameter is mandatory when using trustpool security to ensure that all devices are synchronized.

See the *Cisco IOS Command Reference* for additional details on DHCP configuration.

If DHCP Option 43 is not configured, the device cannot contact the DHCP server, or this method fails for another reason, the network device attempts discovery using DNS. For more information, see [DNS Controller Discovery, on page 370](#).

If the Cisco DNA Center system certificate has an FQDN-only SAN field, you must edit the DHCP pool on the seed device to contain the Option 43 string with FQDN, B2 to B1, dns-server, and domain-name before starting PnP.

If the DHCP pool relies on Cisco switches or routers, a sample configuration is as follows:

```
ip dhcp pool PnP_Pool
network 214.2.64.0255.255.255.0
default-router 214.2.64.1
option 43 ascii "5A1D;B1;K4;I<FQDN>;J80;"
domain-name sitdns.com
dns-server 17.1.104.100
```

DNS Controller Discovery

If DHCP discovery fails to get the IP address of the Cisco DNA Center controller, the network device falls back on the DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the controller, using the preset hostname `pnpserver`. The NTP server name is based on the preset hostname `pnntpserver`.

For example, if the DHCP server returns the domain name “customer.com”, the network device constructs the controller FQDN of `pnpserver.customer.com`. It then uses the local name server to resolve the IP address for this FQDN. The NTP server name FQDN would be `pnntpserver.customer.com`.

The prerequisites for the DNS discovery method are as follows:

- New devices can reach the DHCP server.
- The Cisco DNA Center controller is deployed with the hostname “pnpserver”.
- The NTP server is deployed with the hostname pnpntpserver.

Plug and Play Connect Controller Discovery

In situations where using the DHCP or DNS discovery methods is not an option, the Cisco Plug and Play Connect cloud service allows devices to discover the IP address of the Cisco DNA Center controller. When the network device boots up, if it cannot locate the controller through DHCP or DNS, then it tries Plug and Play Connect by contacting `devicehelper.cisco.com` to obtain the IP address of the appropriate controller that is defined for your organization. To secure the communications, the first thing that the device does when contacting Plug and Play Connect is to download and install the Cisco trustpool bundle.

The following steps summarize how to use Cisco Plug and Play to deploy a Cisco network device by using Plug and Play Connect for discovery.

Before you begin

Cisco network devices are running Cisco IOS images that support Cisco Plug and Play and have connectivity to the Cisco Plug and Play Connect cloud service.

-
- Step 1** The network administrator configures the controller profile for the appropriate Cisco DNA Center controller for your organization by using Plug and Play Connect in the Cisco Smart Account web portal. For more information, see the Smart Account documentation in the web portal.
- Step 2** If you order plug and play network devices through Cisco Commerce Workspace (CCW), these network devices are automatically registered with Plug and Play Connect as long as a Cisco Smart Account is assigned to the order and you include the NETWORK-PNP-LIC option for each device that you want to use with Cisco Plug and Play.
- This option causes the device serial number and PID to be automatically registered in your Smart Account for plug and play. If you have specified a default controller, then the devices are automatically assigned to that controller when the order is processed.
- Step 3** Alternatively, you can manually add devices in the Plug and Play Connect web portal.
- Step 4** Register the Cisco DNA Center controller as a controller for Cisco Plug and Play Connect in a Cisco Smart Account, for redirection services. See [Register or Edit a Virtual Account Profile, on page 376](#).
- This step is required if you order plug and play network devices through CCW and these network devices are automatically registered with Plug and Play Connect through your Smart Account.
- Step 5** Synchronize the device inventory from the Smart Account in the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.
- Devices registered in the Plug and Play Connect web portal are synced to the controller and appear in the plug and play device list with a source of SmartAccount.
- Step 6** Claim the newly synced devices. See [Provision a Device with Plug and Play, on page 378](#).
- Step 7** The device installer installs and powers up the Cisco network device.

Step 8 The device discovers the Cisco DNA Center controller by querying the Plug and Play Connect service, identifies itself by serial number to Plug and Play in Cisco DNA Center, then is provisioned according to what was planned for it during the claim process.



Note The device will fail to contact Plug and Play Connect if the device cannot synchronize with the predefined NTP servers **time-pnp.cisco.com** or **pool.ntp.org**. To resolve this problem, either unblock NTP traffic to these two host names, or map these two NTP host names to local NTP server addresses on the DNS server.

Plug and Play Deployment Guidelines

Follow these recommendations when using Plug and Play:


- **Device bring up order:** In general, routing and upstream devices should be brought up first. Once the router and all upstream devices are up and provisioned, switches and downstream devices can be brought up. The Plug and Play agent in a device attempts to auto-discover the Cisco DNA Center controller only during initial device startup. If at this time, the device cannot contact the controller, device provisioning fails, so upstream devices should be provisioned first.
- **Cisco Router Trunk/Access Port Configuration:** Typical branch networks include routers and switches. One or more switches are connected to the WAN router and other endpoints like IP phones and access points connect to the switches. When a switch connects to an upstream router, the following deployment models are supported for Plug and Play:
 - Downstream switch is connected to the router using a switched port on the router. In this type of connection, the switched port on the router can be configured as a trunk or access port.
 - Downstream switch is connected to the router using a routed port on the router. In this case, the routed port can support multiple VLANs using sub-interfaces. During the Plug and Play process, the switch would automatically configure its port as a trunk port. In a large branch scenario, it becomes necessary to carry multiple VLANs between the router and the downstream switch. To support this use case, the switch must be connected to a routed port.
- **Non-VLAN 1 configuration:** Plug and Play supports devices using VLAN 1 by default. If you want to use a VLAN other than 1, adjacent upstream devices must use supported releases and you must configure the following global CLI command on the upstream device to push this CLI to the upcoming Plug and Play device: **pnp startup-vlan x**. When you execute this command on an adjacent upstream device, the VLAN membership change does not happen on that device. However, the active interfaces on the upcoming Plug and Play device that are connected to the upstream device are changed to the specified VLAN. This guideline applies to both routers and switches and should be used only for trunk mode scenarios and not access mode.

View Devices

You can view information about devices in the **Plug and Play** window.

In addition, you can perform several tasks from this window. For information, see the following topics:

- [Add or Edit a Device, on page 374](#)
- [Add Devices in Bulk, on page 375](#)
- [Add Devices from a Smart Account, on page 377](#)
- [Provision a Device with Plug and Play, on page 378](#)
- [Reset a Device, on page 387](#)
- [Delete a Device, on page 387](#)

Step 1 Click the menu icon () and choose **Provision > Plug and Play**.

The **Plug and Play** window displays a table with the following device information:

Table 32: Device Information


Column	Description
#	Row number.
Device Name	Hostname of the device. Click this link to open the device details window. A stack icon indicates a switch stack.
Serial Number	Device serial number.
Product ID	Device product ID.
IP Address	Device IP address.
Source	Source of the device entry: <ul style="list-style-type: none"> • User: User added the device through the GUI or API. • Network: Unclaimed device that has contacted the controller. • SmartAccount: Device was synced from a Smart Account.
State	<ul style="list-style-type: none"> • Unclaimed: Device has not been provisioned. • Planned: Device has been claimed but has not yet contacted the server. • Onboarding: Device onboarding is in progress. • Provisioned: Device is successfully onboarded and added to inventory. • Error: Device had an error and could not be provisioned.
Onboarding State	Onboarding state of the device. Click on the progress bar to go to the device history.
Site	Site with which the device is associated.
Last Contact	Last date and time the device contacted Plug and Play.
Smart Account	Cisco Smart Account with which the device is associated.

Column	Description
Virtual Account	Virtual Account (within the Cisco Smart Account) with which the device is associated.
Created	Date and time when the device was added to Plug and Play.

The Device table displays the information shown in the following table for each device. Some of the columns support sorting.

- Note**
- Certain columns, such as **Device Name** and **Serial Number**, are displayed in the **Default** focus view.
 - You can customize the **Devices** table to display or hide columns. Click the settings icon (⚙️) to display the **Table Settings** slide-in pane, and from the **Edit Table Columns** tab, choose which columns to display or hide. Click **Apply** to save the changes.

Step 2 From the **Plug and Play** window, you can control the display of device information in the following ways:

- To sort the rows in ascending or descending order, click any column header with a carrot arrow icon .
- To display devices in a particular state, from the **Device Status** filter, choose **Unclaimed**, **Error**, **Provisioned** or **All**.
- To focus the view, from the **Focus** drop-down list, choose **Default** or **All**.
- To change when table information is refreshed, click the **Auto-Refresh** drop-down list and choose the desired auto-refresh time. By default, the devices table refreshes every 30 seconds.
- To find specific devices, use the **Filter** or **Find** option.
- To view device details, click the name of a device.

To view additional details, from the window that opens, click the **Details**, **History**, or **Configuration** tabs. For a switch stack, you can also click the **Stack** tab. Some tabs have additional links that you can click for even more information.

Add or Edit a Device

This procedure shows how to add or edit a device from the Plug and Play Devices list. Alternatively, you can edit a device from the device details window by clicking **Edit**.

Table 33: Device Fields

Field	Description
Serial Number	Device serial number (read only if you are editing a device).
Product ID	Device product ID (read only if you are editing a device).
Device Name	Device name.

Field	Description
Enable SUDI Authorization	Enables secure unique device identifier (SUDI) authorization on devices that support it.
SUDI Serial Numbers	Devices that support SUDI have two serial numbers: the chassis serial number and the SUDI serial number (called the License SN on the device label). Enter one or more comma-separated SUDI serial numbers in this field when adding a device that uses SUDI authorization. This field appears only if Enable SUDI Authorization is checked.
This Device Represents a Stack	Device represents a stack (this item is read only if you are editing a device). Applicable only for supported stackable switches.

Before you begin

If the device requires credentials, be sure that the global device credentials are set in the **Design > Network Settings > Device Credentials** page. For more information, see [Configure Global CLI Credentials, on page 194](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Plug and Play**.
- Step 2** View the devices in the table.
- You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.
- Step 3** Add or edit a device as follows:
- To add a device, click **Add Devices** and then click **Single Device**.
 - To edit a device, check the check box next to the name of the device you want to edit and click **Actions > Edit** in the menu bar above the device table. The **Edit Device** dialog is displayed.
- Step 4** Set the fields as needed, referring to the preceding table for more information.
- Step 5** Save the settings by doing one of the following:
- If you are adding a device and will claim it later, click **Add Device**.
 - If you are adding a device and want to claim it immediately, click **Add + Claim**. For more information on claiming a device, see [Provision a Device with Plug and Play, on page 378](#).
 - If you are editing a device, click **Edit Device**.
-

Add Devices in Bulk

This procedure shows how to add devices in bulk from a CSV file.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Plug and Play**.
- Step 2** Click **Add Devices**.

The **Add Devices** dialog is displayed.

Step 3 Click **Bulk Devices**.

Step 4 Click **Download File Template** to download the file template.

See the file template for information on which fields are mandatory and optional for different devices.

Step 5 Add the information for each device to the file and save the file. Note that certain fields are required, depending on the device type.

Step 6 Upload the CSV file by doing one of the following actions:

- Drag and drop the file to the drag and drop area.
- Click where it says "**click to select**" and select the file.

Step 7 Click **Import Devices**.

The devices in the CSV file are listed in a table.

Step 8 Check the box next to each device to import, or click the check box at the top to select all devices.

Step 9 Add the devices by doing one of the following:

- To add the devices and claim them later, click **Add Devices**.
- To add the devices and claim them immediately, click **Add + Claim**. For more information on claiming a device, see [Provision a Device with Plug and Play, on page 378](#).

Register or Edit a Virtual Account Profile

For redirection services, in a Cisco Smart Account, register Cisco DNA Center as a controller for Cisco Plug and Play Connect. This lets you add the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco Plug and Play in Cisco DNA Center.

You can register a Smart Account, virtual account, and the relevant server profile information with the Plug and Play system and database. The devices in the registered virtual account are synchronized with the Plug and Play database.

Table 34: Virtual Account Fields

Field	Description
Select Smart Account	Cisco Smart Account name.
Select Virtual Account	Virtual account name. Virtual accounts are subaccounts within a Cisco Smart Account.
IP or FQDN	IP address or fully qualified domain name of this Cisco DNA Center controller.
Profile Name	Controller profile name.
Use as Default Controller Profile	<i>Default controller profile</i> means that any new device that is added to a virtual account, or any existing device that doesn't have a default controller assigned, will be assigned to this redirection profile.

-
- Step 1** Click the menu icon (☰) and choose **System > Settings > PnP Connect**.
- Step 2** View the virtual accounts in the table.
- The table lists all of the registered Plug and Play Connect virtual account profiles.
- Step 3** Either register or edit a virtual account profile, as follows:
- To register a virtual account, click **Register**. The Register Virtual Account pane is displayed.
 - To edit a registered virtual account profile, click the radio button next to the name of the profile that you want to edit and click **Edit Profile**. The Edit Profile pane is displayed.
- Step 4** Set the fields as needed.
- Step 5** Save the settings by doing one of the following:
- If you are registering a new virtual account profile, click **Register**.
 - If you are editing a virtual account profile, click **Save**.
-

What to do next

Synchronize the device inventory from the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play. For more information, see [Add Devices from a Smart Account, on page 377](#).

Add Devices from a Smart Account

This task allows you to synchronize the device inventory from a Smart Account in the Cisco Plug and Play Connect cloud portal to Cisco DNA Center Plug and Play.

The Virtual Accounts table displays the following information for each profile.

Table 35: Virtual Accounts Information

Column	Description
Virtual Accounts	Virtual account name.
Smart Accounts	Smart account that the virtual account is associated with.
Profile	Profile name.
Controller	Controller IP address.

Before you begin

Before you can synchronize the device inventory from the Cisco Plug and Play Connect cloud portal, you must register a virtual account. See [Register or Edit a Virtual Account Profile, on page 376](#). You can go directly to the PnP Connect settings page by clicking the **PnP Connect** link in the **Add Devices > Smart Account Devices** dialog.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Plug and Play**.
- Step 2** Click **Add Devices**.
- Step 3** Click **Smart Account Devices**.
- Step 4** If you need to enter a Cisco.com ID (Cisco.com ID shows as Not Associated), do the following:
- Click the **Add** link.
 - Enter the Cisco.com username and password.
 - Click **Save For Later** if you want to save the credentials permanently in Cisco DNA Center, or leave this check box unchecked to use these credentials one time only.
 - Click **Submit**.
- Step 5** Choose the Smart Account and virtual account that you want to register with Plug and Play.
- If you need to register a PnP Connect virtual account profile, click the **PnP Connect** link. If you want to change the Cisco ID, click the **Not me?** link.
- Step 6** From the Devices table, choose the devices that you want to add, and then click **Add Devices**. Added devices appear in the Plug and Play Devices table with the source set to SmartAccount.
-

What to do next

Claim the newly added devices. For more information on claiming a device, see [Provision a Device with Plug and Play, on page 378](#).

Provision a Device with Plug and Play

When you claim a device, you begin the process of provisioning it. When a device is provisioned, Cisco DNA Center performs the following actions:

1. Deploys an image to the device.
2. Deploys system configuration CLI commands that configure the following settings:
 - Device credentials (CLI and SNMP)
 - Enable SSH v2 and SCP server
 - Disable HTTP and HTTPS servers
 - For switches, vtp mode transparent is enabled
3. Deploys a device onboarding configuration template that corresponds to the type of device:
 - For wired devices, Cisco DNA Center deploys the onboarding configuration (Day-0) template that you defined.
 - For wireless devices, Cisco DNA Center deploys a configuration based on the network profile assigned to the site.

If your onboarding configuration template has any of the same system configuration CLI commands, the system configuration CLI commands are overridden, because the onboarding configuration template is applied to the device after the system configuration CLI commands.

4. Adds the device to the inventory.



Note When Device Controllability is enabled for a device (it is enabled by default), additional configurations are pushed to the device when it is added to the inventory or assigned to a site. For more information, see the Device Controllability section in the *Cisco DNA Center Administrator Guide*.

When you claim a device that has not yet booted for the first time, the device is automatically provisioned when it boots up. This process is referred to as device *planning*.

The procedure for provisioning a device depends on the type of device, as follows:

- Switches and routers: See [Provision a Switch or Router Device, on page 379](#)
- Cisco Wireless Controllers, access points, and sensors: See [Provision a Wireless or Sensor Device, on page 383](#)

Provision a Switch or Router Device

This procedure shows how to claim a device from the **Plug and Play Devices** list. Alternatively, you can claim a device from the device **Details** window by clicking **Claim**.

Before you begin

Make sure that the Plug and Play provisioning prerequisites have been met. For information, see [Plug and Play Provisioning Prerequisites, on page 367](#).

Step 1 Click the menu icon (☰) and choose **Provision > Plug and Play**.

Step 2 View the devices in the table.

From the **Focus** drop-down list, choose **Default** or **All** to view the devices.

By default, the devices table gets refreshed every 30 seconds. Click the **Auto-Refresh** drop-down list and choose a refresh time.

Use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to the device or devices that you want to claim.

Step 4 Choose **Actions > Claim** in the menu bar above the device table.

Step 5 (Optional) In the **Assign Site** window, do the following:

- a) Change the device hostname, if needed.
- b) Assign a site by doing any of the following:
 - To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, choose a site.

- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon **...** and choose **Apply Site to All**.
- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon **...** and choose **Assign this Site to Other Devices**, choose the devices, and click **Assign**.
- To clear the site assigned to the devices, click **Clear Site**.

c) Click **Next**.

Step 6

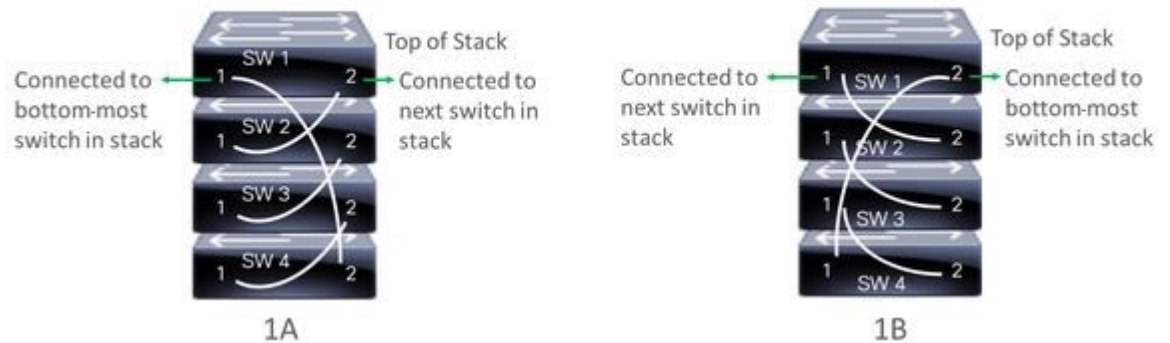
In the **Assign Configuration** window, do the following:

- In the **Configuration** column, click **Assign** for the device that you want to configure.
 - If the device configuration doesn't need any changes, click **Cancel** and proceed to Step 7. Otherwise, change or configure any of the following settings:
 - **Device Name:** Change the device hostname, if needed.
 - **Image:** From this drop-down list, choose a Golden software image to apply to the device. If there is only one Golden image for this device type in the image repository, it is chosen by default.
 - **Template:** From this drop-down list, choose an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.
- Note** If you have not assigned the device to a site, you must choose a template for the device to proceed further.
- **Apply the PKCS12 device certificate on the device:** Check this check box to deploy a PKCS12 certificate to the device. This option is available only for routers.
 - **RTU License Level:** From this drop-down list, choose **Lanbase** or **IP Services**. This option is available only for Cisco Industrial Ethernet (IE) 4000 and 5000 Series Switches.
- Note** To choose **IP Services**, accept the End User License Agreement (EULA) in **System > Settings > Device EULA Acceptance**.
- **Select a Cabling Scheme:** From this drop-down list, choose the stack cabling scheme, if you want to renumber the stack.

This item appears only for switches that support stacking, and only if they are connected, as shown in one of the following cabling schemes.

Figure 20: Cabling Schemes

Supported Stack Switch Wiring Schemes:



- **Select a Top of Stack Serial Number:** The top-of-stack serial number autopopulates with the user-entered stack member serial number. If you don't want to use the autopopulated serial number, click the serial number, and in the **Select a Top of Stack Serial Number** field, click the drop-down arrow. Click the **X** icon to deselect the serial number.

This option appears only for switches that support stacking, and only if they are connected as shown in the preceding image.

For a *planned device*, the top-of-stack serial number is set as the default.

For an *unclaimed device*, the top-of-stack serial number is not set as the default. Choose the top-of-stack serial number from the drop down.

- **Select a License Level:** From this drop-down list, choose the stack license level. Click the **X** icon to deselect the license level.

This item is displayed only for switches that support stacking.

c) Click **Save**.

d) From the **Clear Configuration** drop-down list, choose any the following options:

- **Clear Device Certificates:** Choose this option and check the check box adjacent to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images:** Choose this option and check the check box adjacent to each of the devices that you want to clear the image from, and click **Clear**.
- **Clear Templates:** Choose this option and check the check box adjacent to each of the devices that you want to clear the template from, and click **Clear**.
- **Clear License Levels:** Choose this option and check the check box adjacent to each of the devices that you want to clear the license level from, and click **Clear**.

e) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon **...** and choose **Apply Image to Other Devices** or **Apply Template to Other Devices**.

For stacked devices, you can apply the device license level to other devices by clicking **Apply License Level to Other Devices**.

- f) If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration steps, until you have done this for all devices.
- g) After you have configured all the devices, click **Next**.

Step 7

To configure template parameter values for all the devices in bulk, proceed to Step 8. To configure template parameter values for devices one at a time, from the **Provision Templates** window, do the following:

- a) Click the name of the device that you want to configure.
- b) If the device was assigned a configuration template, specify the values for the parameters that were defined in the template.

Enter the values for each parameter in the fields for each device. A red asterisk indicates a required field.

- c) If you want to copy the running configuration to the startup configuration on the selected device, check the **Copy running config to startup config** check box.
- d) If you selected multiple devices to provision, click the next device in the list at the left side of the window and enter the parameter values, until you have done this for all the devices.
- e) Click **Next**.

Step 8

To specify parameter values for all the devices in bulk, in the **Provision Templates** window, do the following:

- a) Click **Export** to save the CSV template file.
- b) Add the values for each of the parameters to the file and save the file.
- c) Click **Import**.
- d) Drag and drop the file to the drag-and-drop area, or click "**click to select**" and select the file.
- e) Click **Import**.
- f) Click **Next**.

Step 9

In the **Summary** window, view details about the devices and their configuration preview status.

Step 10

Verify the **Day-0 Config** column for each device to see whether the configuration preview was successful.

If the preview shows an error, click the **Actions** link in the error message above the table to see what actions you need to take. You can click an action to open a new tab with the window where a change is needed.

To avoid provisioning errors, resolve issues, if any, before claiming the device. You may need to go back to the **Provision Templates** step and change the parameter values, and the template, revisit the **Design** area to update network design settings, or resolve network connectivity issues, if any.

After you resolve the problem, you can return to **Day-0 Config** column, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**.

Step 11

Click a link in the **Day-0 Config** column to see more information about the device, its configuration, and configuration preview errors, if any.

Step 12

Click **Claim**.

Step 13

In the confirmation dialog box, click **Yes** to claim the devices.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see [Complete the Provisioning Process, on page 386](#).

Provision a Wireless or Sensor Device

This procedure explains how to claim a device from the Plug and Play Devices list. Alternatively, you can claim a device from the device details window by clicking **Claim**.

Before you begin

Make sure that the Plug and Play provisioning prerequisites have been met. For information, see [Plug and Play Provisioning Prerequisites, on page 367](#).

Step 1 Click the menu icon (☰) and choose **Provision > Plug and Play**.

Step 2 View the devices in the table.

You can use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to one or more wireless devices that you want to claim.

Step 4 From the menu bar above the device table, choose **Actions > Claim**.

The **Claim Devices** window opens, showing the first step, **Assign Site**. If, instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click **Add Site** to define a site, and **Add device credentials** to define device credentials. These are prerequisites for the claim process and, after these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device name, if needed, in the first column.

Step 6 (Optional) Change the device type, if needed, in the second column. You can choose AP or ME (Mobility Express), depending on which mode the device is using.

Choosing the wrong mode causes an error provisioning the device. This item does not appear for Cisco Wireless Controller or sensor devices.

Step 7 From the **Select a Site** drop-down list, choose a site and floor to assign to each device. AP devices must be assigned to a floor with a wireless controller.

To apply the same site as the first device to all other devices, check the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**. Wireless devices can be assigned only to floors within a building, not to the building itself.

Note In Release 2.3.5.3, Cisco DNA Center does not configure this site as the AP location during AP PnP onboarding. You can configure the AP location using the **Configure Access Points** workflow. For more information, see [Configure AP Workflow, on page 716](#).

Effective with Release 2.3.5.4, in the **System > Settings > Device Settings > PnP AP Location** window:

- If the **Configure AP Location** check box is checked, Cisco DNA Center assigns this site as the AP location during PnP onboarding.
- If the **Configure AP Location** check box is unchecked, Cisco DNA Center does not configure this site as the AP location during PnP onboarding. You can configure the AP location using the **Configure Access Points** workflow. For more information, see [Configure AP Workflow, on page 716](#).

For more information, see "Configure AP Location for PnP Onboarding" in the [Cisco DNA Center Administrator Guide](#).

Step 8 Click **Next**.

The **Assign Configuration** window opens.

Step 9 (Optional) You can change which columns are displayed in the table by clicking the settings icon (⚙️) in the top-right corner of the table and choosing the desired columns. Click **Apply** to save the changes.

Step 10 In the **Configuration** column, click **Assign** for the device that you want to configure and follow these steps:

- a) View the device configuration summary and click **Cancel** if no changes are needed.
- b) (Optional) In the **Device Name** field, change the device name, if needed.
- c) For an AP device, in the **Radio Frequency Profile** drop-down list, choose a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.
- d) For a wireless controller, enter values in the following fields: **Wireless management IP**, **Subnet mask**, **Gateway**, **IP interface name**, and optionally, **VLAN ID**.
- e) For a Mobility Express device, enter values in the following fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.
- f) For a wireless sensor device, in the **Sensor Settings** drop-down list, choose the sensor device profile (backhaul) to apply to the device.

Note For Cisco Aironet 1800s Active Sensor earlier than Release 1.3.1.2, make sure that you do not choose the sensor device profile **CiscoProvisioningSSID**. Instead, choose your own SSID for backhaul purposes.

- g) If you made any changes, click **Save**; otherwise, click **Cancel** to return to the list and configure other devices.
- h) You can apply a configuration that you assigned to one device to other devices of the same type by clicking **Apply ... to Other Devices** in the **Actions** column.

Step 11 (Optional) For a wireless sensor device, to assign a software image, do the following:

- a. In the **Image** column, click **Assign**.
- b. From the **Image** drop-down list, choose a golden software image.
- c. Click **Save**.

Step 12 If any devices are a Cisco Catalyst 9800-CL Wireless Controller, click **Assign** next to **Image** in the **Configuration** column and follow these steps:

- a) (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.
- b) Click **Save**.

Step 13 If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration, until you have done this for all devices.

Step 14 Click **Next**.

The **Summary** window appears, where you can view details about the devices and configuration.

Step 15 Check the **Day-0 Config** column for each device to see if the configuration preview was successful.

If the preview shows an error, you can click the **Actions** link in the error message above the table to see what actions you need to take. You can click an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Assign Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. After you have resolved the problem, you can go back to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless controller that is managing a device has been added to the inventory and assigned to the site where the wireless device is assigned.

Step 16 Click **Claim**.

Step 17 In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see [Complete the Provisioning Process, on page 386](#).

Provision a Cisco DNA Traffic Telemetry Appliance

This procedure explains how to claim a Cisco DNA Traffic Telemetry Appliance from the Plug and Play Devices list.

Before you begin

Make sure that the Plug and Play provisioning prerequisites have been met. For information, see, [Plug and Play Provisioning Prerequisites, on page 367](#).

Step 1 Click the menu icon (☰) and choose **Provision > Plug and Play**.

Step 2 View the devices in the table.

You can use the **Filter** or **Find** option to find the Cisco DNA Traffic Telemetry Appliance.

Step 3 Check the check box next to one or more devices that you want to claim.

Step 4 From the menu bar above the device table, choose **Actions > Claim**.

The **Claim Devices** window opens, showing the first step, **Assign Site**. If instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click **Add Site** to define a site, and **Add device credentials** to define device credentials. These mandatory tasks are prerequisites for the claim process. After these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device hostname, if needed, in the first column.

Step 6 From the **Select a Site** drop-down list, choose a site to assign to each device.

To apply the same site as the first device to all other devices, check the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**.

Step 7 Click **Next**.

The **Assign Configuration** window appears.

Step 8 In the **Configuration** column, click **Assign** for the device that you want to configure and follow these steps:

- View the device configuration summary and, if no changes are needed, click **Cancel**.
- (Optional) In the **Device Name** field, change the device hostname, if needed.
- (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.
- If you made any changes, click **Save**. Otherwise, click **Cancel** to return to the list and configure other devices.

Step 9 If you selected multiple devices to provision, click **Assign** for the next device in the list. Repeat the configuration steps until you have configured all devices.

Step 10 Click **Next**.

The **Summary** window appears, where you can view details about the devices and their configuration preview status.

- Step 11** Check the **Day-0 Config** column for each device to see if the configuration preview was successful.
- If the preview shows an error, click the **Actions** link in the error message above the table to see what actions you need to take. Click an action to open a new tab with the window where a change is needed. To avoid provisioning errors, you must resolve any issues before claiming the device. You may need to revisit the **Design** area to update network design settings or resolve any network connectivity issues. After you resolve the problem, return to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**.
- Step 12** Click the link in the **Day-0 Config** column to see more information about the device, its configuration, and any configuration preview errors.
- Step 13** Click **Claim**.
- Step 14** In the confirmation dialog box, click **Yes** to claim the devices.
-

What to do next

If you have configured network settings, provision these settings on the devices. For information, see [Complete the Provisioning Process, on page 386](#).

Complete the Provisioning Process

During Plug and Play provisioning, only the device credentials and the onboarding configuration are pushed to the device. No other network settings are pushed. After Plug and Play provisioning is completed, you can complete the provisioning process by pushing the network settings that are configured in the **Design** area.

The network settings include AAA server settings, if these are configured. In the case of Cisco ISE, Cisco DNA Center configures the device on Cisco ISE as a AAA client for RADIUS or TACACS.

For wireless and sensor device, the network settings include wireless settings, such as RF profiles and antenna radio profiles, if these are configured. For more information, see [Wireless Device Provisioning Overview, on page 389](#).

Before you begin

- Ensure that the device has been provisioned (onboarded) using one of the following procedures:
 - [Provision a Switch or Router Device, on page 379](#)
 - [Provision a Wireless or Sensor Device, on page 383](#)
 - Configure network settings. For information, see [Configure Network Settings, on page 191](#).
-

- Step 1** In the Cisco DNA Center GUI, click the menu icon (☰) and choose **Provision > Inventory**.
- Step 2** Select the device and choose **Actions > Provision > Provision Device**.
- Step 3** Proceed through the steps in the workflow.
- Step 4** In the **Summary** window, review the remaining network settings. To make any changes, click **Edit** next to the relevant category; otherwise, click **Deploy**.
-

Delete a Device

Deleting a device removes it from the Plug and Play database but does not reset the device. Use **Reset** if you want to reset a device that is in the Error state.

This procedure explains how to delete a device from the Plug and Play Devices list. Alternatively, you can delete a device from the device details window by clicking **Delete**.



Note If a device is in the Provisioned state, it can be deleted only from the **Inventory** tab.

Step 1 Click the menu icon (☰) and choose **Provision > Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Check the check box next to one or more devices that you want to delete.

Step 4 From the menu bar above the device table, choose **Actions > Delete**.

Step 5 Click **Yes** to confirm that you want to delete the devices.

Reset a Device

Resetting a device applies only to devices in the Error state and resets its state to Unclaimed and reloads the device, but does not remove it from the Plug and Play database. Use **Delete** if you want to delete a device.



Note If the saved configuration on the device is the factory default or a similar minimal configuration, then this option causes the device to restart the provisioning process. However, if the device has a previously saved startup configuration, then this could prevent the device from restarting the provisioning process and it will need to be reset to factory defaults. On wireless and sensor devices, only the device state is reset and the device is not reloaded.

This procedure shows how to reset a device from the Plug and Play Devices list. Alternatively, you can reset it from the device details window by clicking **Reset**.

Step 1 Click the menu icon (☰) and choose **Provision > Plug and Play**.

Step 2 View the devices in the table.

You can filter on device state by using one of the **Device State** buttons, or use the **Filter** option to find specific devices. Click **Refresh** to refresh the device list.

Step 3 Check the check box next to one or more devices that you want to reset.

Step 4 Click **Actions > Reset** in the menu bar above the device table.

A confirmation dialog box is displayed.

Step 5 Choose one of the following options:

- **Reset and keep current claim parameters**—Keep the current claim parameters and the device goes to the Planned state.
- **Reset and remove all claim parameters**—Remove the current claim parameters and the device goes to the Unclaimed state.

Step 6 Click **Reset**.



CHAPTER 17

Provision Wireless Devices

- [Wireless Device Provisioning Overview](#), on page 389
- [About Wireless Devices and Country Codes](#), on page 389
- [Prerequisites for Provisioning a Cisco AireOS Controller](#), on page 390
- [Provision a Cisco AireOS Controller](#), on page 391
- [Provision a Cisco AP—Day 1 AP Provisioning](#), on page 397
- [Enable ICMP Ping on APs in FlexConnect Mode](#), on page 399
- [Day 0 Workflow for Cisco AireOS Mobility Express APs](#), on page 399
- [Provision Cisco AireOS Controllers in the Existing Deployment](#), on page 401
- [Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller](#), on page 403
- [Configure and Provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches](#), on page 431
- [Inter-Release Controller Mobility Introduction](#), on page 437
- [Prerequisites for Provisioning a Meraki Device](#), on page 440
- [Provision a Meraki Device](#), on page 441
- [Provision Remote Teleworker Devices](#), on page 443

Wireless Device Provisioning Overview

The following sections provide information about how to provision various Cisco wireless devices.

About Wireless Devices and Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation within that regulatory domain (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Cisco DNA Center provisions controllers with country codes according to the site they are assigned. In the case of controllers, they can be assigned to more than one site. So, they can be assigned more than one country code. During provisioning, Cisco DNA Center assigns sites to the controller along with the sites' country codes. For example, a controller that manages both India and US sites is assigned the IN and US country codes.

When access points are provisioned, they are assigned to a floor. If the access point is a ROW AP, Cisco DNA Center gets the country code for the site and assigns it to the AP. Any additional APs on the same floor are assigned the same country code.

During AP provisioning with an RF profile selected, out of all the Dynamic Channel Assignment (DCA) channels configured on the RF profile, only the supported channels as per the country code are considered. You can see the list of unsupported DCA channels in the AP preprovision summary step of the AP provision workflow on Cisco DNA Center.

The country code information is displayed on the **Device 360** window for controllers and access points.

For a complete list of country codes supported per product, see

<https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html>.

Prerequisites for Provisioning a Cisco AireOS Controller

- Make sure that you have defined the following global network settings before provisioning a Cisco Wireless Controller:
 - Network servers, such as AAA, DHCP, and DNS.
For more information, see [Configure Global Network Servers, on page 193](#).
 - Device credentials, such as CLI, SNMP, HTTP, and HTTPS.
For more information, see [Configure Global CLI Credentials, on page 194](#), [Configure Global SNMPv2c Credentials, on page 195](#), [Configure Global SNMPv3 Credentials, on page 195](#), and [Configure Global HTTPS Credentials, on page 197](#).
 - IP address pools.
For more information, see [Configure IP Address Pools, on page 202](#).
 - Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles.
For more information, see [Configure Global Wireless Settings, on page 207](#).
- Make sure that you have the Cisco Wireless Controller in your inventory. If not, use the **Discovery** feature to discover the controller.
- Make sure that the Cisco Wireless Controller is added to a site. For more information, see [Add a Device to a Site, on page 90](#).
- You cannot reuse any pre-existing VLANs on devices. Provisioning fails if Cisco DNA Center pushes the same VLAN that already exists on the device.
- You cannot make any configuration changes to the wireless controller that is being managed by the Cisco DNA Center manually. You must perform all configurations from the Cisco DNA Center GUI.

Provision a Cisco AireOS Controller

Before you begin

Ensure the prerequisite is met. For more information, see [Prerequisites for Provisioning a Cisco AireOS Controller, on page 390](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window is displayed with the discovered devices listed.
- Step 2** Expand the **Global** site in the left pane, and select the site, building, or floor that you are interested in.
The available devices in the selected site is displayed in the **Inventory** window.
- Step 3** From the **DEVICE TYPE** list, click the **WLCs** tab, and from the **Reachability** list, click the **Reachable** tab to get the list of wireless controllers that are discovered and reachable.
- Step 4** Check the check box next to the device name that you want to provision.
- Step 5** From the **Actions** drop-down list, choose **Provision > Provision Device**.
The **Assign Site** window is displayed.
- Step 6** Click **Choose a site** to assign a site for the wireless controller.
- Step 7** In the **Add Sites** window, check the check box next to the site name to associate the wireless controller, and click **Save**.
- Step 8** Click **Apply**.
- Step 9** Click **Next**.
The **Configuration** window is displayed.
- Step 10** Select a role for the wireless controller: **Active Main WLC** or **Guest Anchor WLC**.
- Step 11** Click **Select Primary Managed AP Locations** to select the managed AP location for the wireless controller.
- Step 12** In the **Managed AP Location** window, check the check box next to the site name. You can either select a parent site or the individual sites. If you select a parent site, the children under that parent site are automatically selected.
- Note** Inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that site. One wireless controller can manage only one site.
- Step 13** Click **Save**.
- Step 14** (Optional) Check the **AP Authorization List** check box to choose the authorization list for AP authorization, and do the following:
- Note** This check box is displayed only if an AP authorization list is available. For more information about AP authorization list, see [Create an AP Authorization List, on page 250](#).
- From the **AP Authorization List Name** drop-down list, choose an AP authorization list. Based on the content of the AP authorization list, Cisco DNA Center displays a message indicating the corresponding primary authorization type and failback mechanism.
 - (Optional) To view the entries for the selected AP authorization list, click **View Entries**.

- If the wireless controller manages both mesh and nonmesh APs, Cisco DNA Center displays the **Authorize Only Mesh Access Points** and **Authorize All Access Points** check boxes.

To enable authorization for only mesh APs, check the **Authorize Only Mesh Access Points** check box.

To enable authorization for all APs, check the **Authorize All Access Points** check box.

Step 15 Under **Interface and VLAN Configuration**, click + **Add** and configure the interface and VLAN details for an active main wireless controller.

Interface and VLAN configuration is applicable for nonfabric wireless controller provisioning only.

The **Configure Interface and VLAN** window is displayed.

Step 16 From the **Interface Name** drop-down list, choose the interface name.

Step 17 In the **VLAN ID** field, enter a value for the VLAN.

Step 18 In the **Interface IP Address** field, enter a value for the interface IP address.

Step 19 In the **Interface Net Mask (in bits)** field, enter the subnet mask for the interface.

Step 20 In the **Gateway IP Address** field, enter the gateway IP address.

Step 21 From the **LAG/Port Number** drop-down list, choose the link aggregation or the port number.

Step 22 Click **OK**.

Step 23 (Optional) For a guest anchor wireless controller, change the VLAN ID configuration by changing the **VLAN ID** under **Assign Guest SSIDs to DMZ site**.

Step 24 Under **Mobility Group**, click **Configure** to configure the wireless controller as the mobility peer.

Step 25 In the **Configure Mobility Group** slide-in pane, from the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking +, or choose a mobility group from the existing mobility groups.

Information about the existing mobility peers is loaded from the intent available in the Cisco DNA Center.

Note If you choose the default mobility group from the drop-down list, you cannot add mobility peers.

Step 26 In the **RF Group Name** text box, enter a name for the RF group.

Step 27 Under **Mobility Peers**, click **Add** to configure the wireless controller as a mobility peer.

Step 28 In the **Add Mobility Peer** slide-in pane, configure the following:

a) Choose one of the following types of mobility peers:

- To include mobility peers that are managed by Cisco DNA Center, click **Managed WLC**.
- To include mobility peers that are not managed by Cisco DNA Center, click **External WLC**.

b) If you choose **Managed WLC**, from the **Device Name** drop-down list, choose the controller.

After the device is provisioned, Cisco DNA Center creates a mobility group in device, assigns the RF group, and configures all ends of peers. The mobility group configuration is deployed automatically to all the selected peer devices.

c) If you choose **External WLC**, configure the following:

- In the **Device Name** field, enter the device name.
- (Optional) From the **Device Series** drop-down list, choose the device series.
- In the **Public IP Address** field, enter the public IP address.

- (Optional) In the **Private IP Address** field, enter the private IP address.
- In the **MAC Address** field, enter the MAC address of the device.
- In the **Mobility Group Name** field, enter the mobility group name.
- (Optional) In the **Hash** field, enter the hash for the Cisco Catalyst 9800 Series Wireless Controller.

Note This field is available only for Cisco Catalyst 9800-CL Wireless Controller.

d) Click **Save**.

Step 29 Click **Configure Mobility**.

Step 30 To reset the mobility group name and the RF group name, you can do one of the following:

- In the **Configure Mobility Group** slide-in pane, choose **default** from the **Mobility Group Name** drop-down list.
- In the **Configure Mobility Group** slide-in pane, click **Reset Mobility**.
- On the **Provision > Configuration** window, under **Mobility Group**, click **Reset**.

This automatically sets the **RF Group Name** to **default** and removes all peers. After provisioning, the mobility on the device is set and the device is removed from all other peers.

Step 31 Click **Next**.

The **Model Configuration** window is displayed.

Step 32 In the **Devices** pane, you can either search for a model config design by entering its name in the **Find** field, or expand the device and select a model configuration design.

The selected model configuration design is displayed in the right pane.

Step 33 Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the model configuration design.

You cannot edit all the configurations at this step.

Step 34 After making the necessary changes, click **Apply**.

Step 35 Click **Next**.

The **Advanced Configuration** window is displayed, which is where you can enter the values for predefined template variables.

Step 36 Search for the device or the template in the **Devices** panel.

Step 37 Enter a value for the predefined template variable in the **wlanid** field.

Step 38 Click **Next**.

Step 39 Click **Deploy** to provision the controller.

Step 40 In the **Provision Devices** window, do the following to preview the CLI configuration:

- a) Click the **Generate Configuration Preview** radio button.
- b) In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- c) In the **Task Submitted** dialog box, click the **Work Items** link.

Note This dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon (☰) and choose **Activities > Work Items**.

- d) In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- e) View the CLI configuration details and click **Deploy**.
- f) To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- g) To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- h) In the **Information** dialog box, do the following:
 1. Click **Yes**, if you want to delete the CLI preview task from the **Work Items** window.
 2. Click **No**, if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Step 41 Provision the secondary controller.

Step 42 The **Status** column in the **Device Inventory** window shows *SUCCESS* after a successful deployment.

After provisioning, if you want to make any changes, click **Design**, change the site profile, and provision the wireless controller again.

Step 43 After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 44 In the **Device Inventory** window, click **See Details** in the **Provision Status** column to get more information about the network intent or to view a list of actions that you need to take.

Step 45 Click **See Details** under **Device Provisioning**.

Step 46 Click **View Details** under **Deployment of network intent**, and click the device name.

Step 47 Expand the **Configuration Summary** area to view the operation details, feature name, and the management capability. The configuration summary also displays any errors that occurred while provisioning the device.

Step 48 Expand the **Provision Summary** area to view details of the exact configuration that is sent to the device.

Configure Cisco Wireless Controller High Availability

Cisco Wireless Controller High Availability (HA) can be configured through Cisco DNA Center. Currently, both the formation and breaking of wireless controller HA is supported; switchover options are not supported.

Prerequisites for Configuring Cisco Wireless Controller High Availability

- The Discovery and Inventory features of wireless controller 1 and wireless controller 2 must be successful. The devices must be in the Managed state.
- The service ports and the management ports of wireless controller 1 and wireless controller 2 must be configured.
- The redundancy ports of wireless controller 1 and wireless controller 2 must be physically connected.
- The management address of wireless controller 1 and wireless controller 2 must be in the same subnet. The redundancy management address of wireless controller 1 and wireless controller 2 must also be in the same subnet.
- Manually configure the following boot variables on the wireless controller:

```

config t
boot system bootflash:<device_iosxe_image_filename>
config-register 0x2102

show boot. (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102

```

Configure Cisco Wireless Controller HA

- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window is displayed with the discovered devices listed.
- Step 2** Check the check box next to the controller name that you want to configure as the primary controller.
- Step 3** From the **Actions** drop-down list, choose **Provision > Configure WLC HA**.
The **High Availability** slide-in pane is displayed.
- Step 4** Enter the **Redundancy Management IP** and the **Peer Redundancy Management IP** address in the respective text boxes.
The IP addresses used for redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the Cisco Wireless Controller. Ensure that these IP addresses are unused IP addresses within that subnet range.
- Step 5** From the **Select Secondary WLC** drop-down list, choose the secondary controller.
- Note** When you choose the secondary controller, based on the wireless management interface IP subnet of the primary controller, the redundancy management IP is auto populated, and an **i** icon is displayed at the top of the **High Availability** window, along with the following message:
Please make sure the Redundancy Management IP and Peer Redundancy Management IP are not assigned to any other network entities. If used, kindly change the IP accordingly and configure.
- Step 6** Click **Configure HA**.
The HA configuration is initiated in the background using the CLI commands. First, the primary wireless controller is configured. On success, the secondary wireless controller is configured. After the configuration is complete, both wireless controllers reboot. This process may take up to 2.5 minutes to complete.
- Step 7** To verify the HA configuration, on the **Devices > Inventory** window, click the device that you configured as a HA device.
- Step 8** Click the **Wireless Info** tab.
The **Redundancy Summary** displays the **Sync Status** as **In Progress**. When Cisco DNA Center finds that HA pairing succeeded, the **Sync Status** changes to **Complete**.
This is triggered by the inventory poller or manual resynchronization. By now, the secondary wireless controller (wireless controller 2) is deleted from Cisco DNA Center. This flow indicates a successful HA configuration on the wireless controller.
-

What Happens During or After the High Availability Process is Complete

1. Cisco wireless controller 1 and wireless controller 2 are configured with redundancy management, redundancy units, and SSO. The wireless controllers reboot in order to negotiate their role as active or standby. Configuration is synced from active to standby.
2. On the **Show Redundancy Summary** window, you can see these configurations:
 - SSO is enabled.
 - The wireless controller is active.
 - The wireless controller is in hot standby.
3. The management port of the active wireless controller is shared by both the controllers and will be pointing to the active controller. The user interface, Telnet, and SSH on the standby wireless controller will not work. You can use the console and service port interface to control the standby wireless controller.

Commands to Configure and Verify High Availability

Cisco DNA Center sends the following commands to configure Cisco Wireless Controller HA.

Cisco DNA Center sends the following commands to wireless controller 1:

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Cisco DNA Center sends the following commands to wireless controller 2:

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

Enter the following commands to verify the HA configuration from the wireless controller:

- To check HA-related details: **config redundancy mode sso**
- To check the configured interfaces: **show redundancy summary**

Disable High Availability Configured Device in the Existing Deployment

The Cisco DNA Center Disable HA feature is supported on Cisco Catalyst 9800 Series Wireless Controllers and Cisco AireOS Controllers.

Before you begin

Ensure that the HA device in the existing deployment is configured outside of Cisco DNA Center.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Device > Inventory**.
The **Inventory** window is displayed with the discovered devices listed.
- Step 2** Check the check box next to the name of the wireless controller that has the HA feature that you want to disable.
- Step 3** From the **Actions** drop-down list, choose **Provision > Configure WLC HA**.
The **High Availability** slide-in pane is displayed.
High Availability slide-in pane shows the **REDUNDANCY SUMMARY** of selected wireless controller configured from outside Cisco DNA Center.
- Step 4** In the **Warning** window, click **OK**.
A success message appears at the bottom of the screen indicating that the HA feature has been successfully disabled for the selected wireless controller.
-

Provision a Cisco AP—Day 1 AP Provisioning

Before you begin

- Make sure that you have Cisco APs in your inventory. If not, use the Discovery feature to discover APs. For more information, see [Discover Your Network, on page 37](#).
- If you add new AP zones or SSIDs, you must reprovision the wireless controller. For more information, see [Provision a Cisco AireOS Controller, on page 391](#) and [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).
- If you update the AP zone configurations, you must reprovision the wireless controller. For more information, see [Provision a Cisco AireOS Controller, on page 391](#) and [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window displays the device information that is gathered during the Discovery process.
- Note** You can either search for a site by entering its name or expand **Global** to select the site. Devices that are available in the selected site are displayed in the **Inventory** window.
To filter the devices based on various criteria, such as **Device Family** or **Reachability Status**, click **Filter**, make your selections, then click **Apply**.
- Step 2** Check the check box next to the AP that you want to provision.
- Step 3** From the **Action** drop-down list, choose **Provision > Provision Device**.
- Step 4** In the **Assign Site** step, configure the following parameters:
- a) Click **Choose a floor** and assign an AP to the site.
 - b) In the **Choose a floor** slide-in pane, select the floor where the AP resides, and click **Save**.

c) Click **Next**.

Note Cisco DNA Center does not configure this site as the AP location during AP provision. You can configure the AP location using the **Configure Access Points** workflow. For more information, see [Configure AP Workflow](#), on page 716.

Step 5 In the **Configuration** step, configure the following parameters:

a) Click **Advanced Configuration** to configure radio antenna profiles on antenna slots.

Note Advanced configuration is supported on Cisco Catalyst 9130AXE Unified Access Points with Cisco Catalyst 9800 Series Wireless Controller software release 17.6 or later.

b) Configure the beam selection value for AP radio slot 1 and slot 2 from the **Slot 1** and **Slot 2** drop-down list.

c) Click **Save**.

d) From the **AP Zone Name** drop-down list, choose an AP zone.

Note This drop-down list is enabled only when AP zones are added to the network profile for the site.

If you choose an AP zone, the RF profile is inherited from the AP zone configuration.

e) From the **RF Profile** drop-down list, use the default settings or choose a different value from the list.

The default RF profile is the custom profile that you marked as default under **Design > Network Settings > Wireless > Wireless Radio Frequency Profile**.

Note This drop-down list is disabled if you choose an AP zone from the **AP Zone** drop-down list.

f) In the **Mesh Role** drop-down list, choose **Root** or **Mesh**.

g) Click **Next**.

Step 6 In the **Summary** step, review the device details, and click **Deploy** to provision the AP.

The **Provision Device** slide-in pane appears.

Step 7 In the **Provision Device** slide-in pane, do the following:

- To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- To preview the CLI configuration, click the **Generate Configuration Preview** radio button.

Step 8 You are prompted with a message that creation or modification of an AP group is in progress, and then a message that APs will reboot after provisioning. Click **OK**.

The **Last Sync Status** column in the **Inventory** window shows `SUCCESS` for a successful deployment.

Enable ICMP Ping on APs in FlexConnect Mode

You can enable Internet Control Message Protocol (ICMP) ping on APs that are in FlexConnect mode and in an unreachable state. Cisco DNA Center uses the ICMP to ping FlexConnect APs that are in unreachable state every 5 minutes to enhance reachability and then updates the reachability status in the **Inventory** window.

-
- Step 1** Click the menu icon (☰) and choose **System > Settings > Device Settings > ICMP Ping**.
- Step 2** Check the **Enable ICMP ping for unreachable access points in FlexConnect mode** check box to enable the ICMP ping.
- Step 3** Click **Save**.
- A success message is displayed: ICMP Ping status updated successfully.
- Cisco DNA Center starts pinging FlexConnect APs that are disassociated from Cisco Wireless Controllers but are reachable. You can view the reachability status in the **Inventory** window.
- Step 4** To view the reachability status, choose **Provision > Inventory**.
- Step 5** The **Reachability** column shows **Ping Reachable** when the device is reachable by the ICMP ping.
-

Day 0 Workflow for Cisco AireOS Mobility Express APs

Before you begin

The Cisco Mobility Express wireless network solution comprises at least one 802.11ac Wave 2 Cisco Aironet Series access point with an in-built, software-based wireless controller managing other APs in the network. The AP acting as the wireless controller is referred to as the *primary AP*. The other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as *subordinate APs*.

- Design your network hierarchy with sites, buildings, floors, and so on. For more information, see [Create, Edit and Delete a Site, on page 134](#), [Add, Edit, and Delete a Building, on page 135](#), and [Add, Edit, and Delete a Floor, on page 136](#).
- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS at the global level. The credentials that are defined at the global level are inherited by the sites. For more information, see [Configure Global CLI Credentials, on page 194](#), [Configure Global SNMPv2c Credentials, on page 195](#), and [Configure Global SNMPv3 Credentials, on page 195](#).
- Create WLANs, interfaces, and RF profiles.
- Configure the DHCP server with Option #43 or Option #60. This is the IP address of the Cisco DNA Center Plug and Play server. Using this IP address, the APs contact the PnP server and download the configuration.
- Make sure that you have Mobility Express APs in the inventory. If not, discover them using the Discovery feature. For more information, see [Discover Your Network Using CDP, on page 46](#), [Discover Your Network Using an IP Address Range or CIDR, on page 48](#), and [About Inventory, on page 56](#).
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

-
- Step 1** The Cisco Mobility Express contacts the DHCP server and connects to the Cisco DNA Center Plug and Play server.
- Step 2** The DHCP server allocates the IP address with Option #43, which is the IP address of the Cisco DNA Center Plug and Play server.
- Step 3** The Mobility Express AP starts the PnP agent and contacts the PnP server.
- Note** If you have a set of Mobility Express APs in the network, they go through an internal protocol. The protocol selects one Mobility Express AP, which will be configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.
- Step 4** Find the unclaimed AP in the **Provision > Network Devices > Plug and Play** tab.
- The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.
- You must wait for the **Onboarding Status** to become **Initialized**.
- Step 5** To claim the AP, check the check box next to the AP device name.
- Step 6** Choose **Actions > Claim** in the menu bar above the device table.
- The **Claim Devices** window is displayed.
- Step 7** In the **Site Assignment** window, choose a site from the **Site** drop-down list.
- Claiming the selected AP to this particular site also applies the associated configurations.
- Step 8** Click **Next**.
- Step 9** To configure a device, click the device name in the **Configuration** window.
- Step 10** In the **Configuration for device name** window, assign the static IP details for the device:
- **Management IP**
 - **Subnet Mask**
 - **Gateway**
- Step 11** Click **Save**.
- Step 12** Click **Next**.
- The **Summary** window is displayed.
- Step 13** Click **Claim** in the **Summary** window.
- After the Mobility Express AP is claimed, the configured IP address is assigned to the Mobility Express AP.
- The claimed device, which is an AP, and the wireless controller are now available under **Provision > Device Inventory > Inventory**.
- Step 14** (Optional) Add devices in bulk from a CSV file.
- For more information, see [Add Devices in Bulk, on page 375](#).
- When you bulk import Mobility Express APs through a CSV file, all the Mobility Express APs appear on the **Devices > Plug and Play** window. Based on the VRRP protocol, only one Mobility Express AP among the imported ME APs becomes the primary AP. The remaining APs become subordinate APs. After claiming the primary AP, you don't need to claim the subordinate APs. Cisco DNA Center does not clear the subordinate APs from the **Plug and Play** window. You must delete those subordinate APs manually from the **Devices > Plug and Play** window.

Step 15 To provision the Cisco Wireless Controller, see [Provision a Cisco AireOS Controller, on page 391](#).

Provision Cisco AireOS Controllers in the Existing Deployment

Before you begin

With Cisco DNA Center, you can add and provision the Cisco Wireless Controller, which belongs to existing sites with pre-existing infrastructure.

- Start by running a Discovery job on the device. All your devices are displayed on the **Inventory** window. For more information, see [Discover Your Network, on page 37](#) and [About Inventory, on page 56](#).
 - The wireless controller should be reachable and in the Managed state on the **Inventory** window. For more information, see [About Inventory, on page 56](#).
-

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window is displayed with the discovered devices listed.

Step 2 Click **Filter** and enter the appropriate values in the selected filter field. For example, for the **Device Name** filter, enter the name of the device.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

Step 3 Check the check box next to the wireless controller device name that you want to provision.

Step 4 From the **Actions** drop-down list, choose **More > Learn Device Config**.

The **Site Assignment** window opens and the **Learn Device Configuration** workflow begins.

Note You can also start this workflow by doing the following:

- a. From the **Inventory** window, click the device's link to open a pop-up window that provides high-level information for that device.
- b. Click **View Device Details** to open the device's details page.
- c. Click **Learn WLC Config**.

Step 5 Associate a site to the controller in the **Assign Site** step:

- a) Click **Choose a site** to assign a site to the controller.
- b) In the **Choose a site** slide-in pane, select a site to which you want to associate the wireless controller, and click **Save**.
- c) Click **Next**.

Step 6 The **Resolve Conflict** step shows any conflicting configurations in Cisco DNA Center that you need to resolve.

Step 7 Click **Next**.

Step 8 The **Design Object** window lists all the learned configurations.

- a) Click **Network** in the left pane.

The right pane displays network configurations that were learned as a part of device configuration learning and shows the following information:

- **AAA Server** details.
- **Systems Settings**, with details about the IP address and protocol of the AAA server.
- **DHCP Server** details.
- Enter the **Shared Secret** for the AAA server.

b) Click **Wireless** in the left pane.

The right pane lists the enterprise SSIDs, guest SSIDs, antenna radio profiles, and wireless interface details.

For an SSID with a preshared key (PSK), enter the **passphrase key**.

c) Click **Discarded Config** in the left pane.

The right pane lists the conflicting or the existing configurations on Cisco DNA Center. The discarded configuration entries are categorized as:

- Duplicate design entity
- Unknown device configuration for Radio Policy

d) Click **Next**.

The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

e) Click **Save**.

Step 9 Choose **Design > Network Profiles** to assign a site to the network profile.

Step 10 In the **Network Profiles** window, configure the following:

- a) Click **Assign Site** to add sites to the selected profile.
- b) In the **Add Sites to Profile** window, choose a site from the drop-down list, and click **Save**.

Step 11 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

a) Click **Filter** to locate the device that you want to provision.

The data that is displayed in the **Devices** table is automatically updated according to your filter selection.

- b) Check the check box next to the controller device name that you want to provision.
- c) From the **Actions** drop-down list, choose **Provision**.
- d) Review the details in the **Assign Site** window, and click **Next**.

The **Configurations** step is displayed.

- e) Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.
- f) In the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.
- g) Click **Next**.

Step 12 In the **Summary** window, review the configuration settings.

Step 13 Click **Deploy**.

Step 14 In the **Provision Devices** slide-in pane, do the following to preview the CLI configuration:

- a) Click the **Generate Configuration Preview** radio button.

- b) In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- c) In the **Task Submitted** dialog box, click the **Work Items** link.

Note This dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon (☰) and choose **Activities > Work Items**.

- d) In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- e) View the CLI configuration details and click **Deploy**.
- f) To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- g) To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- h) In the **Information** dialog box, do the following:
 1. Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
 2. Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Configure and Provision a Cisco Catalyst 9800 Series Wireless Controller

Cisco Catalyst 9800 Series Wireless Controller Overview

The Cisco Catalyst 9800 Series Wireless Controller is the next generation of wireless controllers built for intent-based networking. The Cisco Catalyst 9800 Series Wireless Controller is Cisco IOS XE based and integrates the RF excellence from Aironet with the intent-based networking capabilities of Cisco IOS XE to create the best-in-class wireless experience for your organization.

The Cisco Catalyst 9800 Series Wireless Controller is built on a modular operating system and uses open, programmable APIs that enable automation of day-0 and day-N network operations.

The Cisco Catalyst 9800 Series Wireless Controller is available in multiple form factors:

- Catalyst 9800-40 Wireless Controller.
- Catalyst 9800-80 Wireless Controller.
- Catalyst 9800-CL Cloud Wireless Controller: Deployable on private cloud (ESXi, KVM, Cisco ENCS, and Hyper-V) and manageable by Cisco DNA Center.
- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches, Catalyst 9400 Series Switches, and Catalyst 9500H Series Switches.
- Cisco Catalyst 9800-L Wireless Controller: Provides seamless software updates for small- to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network.

The following table lists the supported virtual and hardware platforms for the Cisco Catalyst 9800 Series Wireless Controller:

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	<p>Supports up to 6000 access points and 64,000 clients.</p> <p>Supports up to 80 Gbps throughput and occupies a 2-rack unit space.</p> <p>Modular wireless controller with up to 100-GE uplinks and seamless software updates.</p>
Cisco Catalyst 9800-40 Wireless Controller	<p>A fixed wireless controller with seamless software updates for mid-sized organizations and campus deployments.</p> <p>Supports up to 2000 access points and 32,000 clients.</p> <p>Supports up to 40 Gbps throughput and occupies a 1-rack unit space.</p> <p>Provides four 1-GE or 10-GE uplink ports.</p>
Cisco Catalyst 9800-CL Cloud Wireless Controller	<p>Cisco Catalyst 9800-CL Cloud Wireless Controller can be deployed in a private cloud or a public cloud as Infrastructure as a Service (IaaS).</p> <p>Cisco Catalyst 9800-CL Cloud Wireless Controller is the next generation of enterprise-class virtual wireless controllers built for high availability and security.</p> <p>A virtual form factor of Cisco Catalyst 9800-CL Cloud Wireless Controller for private cloud supports ESXi, KVM, Cisco ENCS, and Hyper-V hypervisors.</p>
Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches	<p>Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches bring the wired and wireless infrastructure together with consistent policy and management.</p> <p>This deployment model supports only Cisco SD-Access, which is a highly secure solution for small campuses and distributed branches. The embedded controller supports access points (APs) only in Fabric mode.</p>
Cisco Catalyst 9800-L Wireless Controller	<p>Cisco Catalyst 9800-L Wireless Controller provides seamless software updates for small to mid-size enterprises. The Cisco Catalyst 9800-L Wireless Controller is available in two variations. You can choose between copper and fiber uplinks, which gives you flexibility in your network.</p> <ul style="list-style-type: none"> • Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45) • Cisco Catalyst 9800-L Fiber Series Wireless Controller 9800-L-F SFP)

The following table lists the host environments supported by the Cisco Catalyst 9800 Series Wireless Controller:

Host Environment	Software Version
VMware ESXi	<ul style="list-style-type: none"> • VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5³ • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5

Host Environment	Software Version
KVM	<ul style="list-style-type: none"> Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2 Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 and 3.9.1

³ Installing the .ova file of C9800-CL using ESXi vSphere does not work. This is not limited to the C9800 ova but affects other products. Cisco and VMware are actively working to fix the issue. Contact your Cisco account representative to see if the problem is fixed. There are issues specific to VMware 6.5 and C9800-CL OVA file deployment in which deployment fails with the warning "A required disk image was missing" and the error "Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files." To install C9800-CL on VMware ESXi 6.5, do one of the following: 1) Install the .iso file of C9800-CL using the ESXi embedded GUI (ESXi 6.5 client version 1.29.0 is tested and required). 2) Install the .ova file of C9800-CL using the OVF tool.

The following table lists the Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) versions supported in Cisco DNA Center:



Note Cisco Enterprise NFVIS devices support the N-1 to N upgrade path only. For example, upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 3.12.x only is supported. Upgrade from Cisco Enterprise NFVIS 3.11.x to Cisco Enterprise NFVIS 4.1.x is not supported.

Cisco Enterprise NFVIS Version	Enterprise Network Compute System Device Platform	Notes
4.1.2 4.1.1 3.12.3 3.11.3 3.11.2 3.11.1	ENCS 5400 UCS-E UCS-C	<p>Cisco DNA Center supports the following NFVIS upgrade paths: NFVIS v3.11.1 > 3.11.2 > 3.11.3 > 3.12.3 > 4.1.1 > 4.1.2.</p> <p>Cisco Enterprise NFVIS 3.12.1 is not supported on any versions of Cisco DNA Center.</p> <p>Upgrade to Cisco Enterprise NFVIS 3.12.1 from Cisco Enterprise NFVIS 3.11.x using Cisco DNA Center is not supported.</p> <p>Upgrade to Cisco Enterprise NFVIS 3.12.2 from Cisco Enterprise NFVIS 3.12.1 using Cisco DNA Center is not supported.</p> <p>Upgrade to Cisco Enterprise NFVIS 3.12.2 from 3.11.2 is supported using Cisco DNA Center.</p> <p>Cisco Enterprise NFVIS 3.12.2 is supported on Cisco DNA Center.</p>
3.12.2 3.11.3 3.11.2 3.11.1	ENCS 5100	Cisco 5100 ENCS does not support Cisco Enterprise NFVIS 3.10.x.

Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center

1. Install Cisco DNA Center.
For more information, see the [Cisco DNA Center Installation Guide](#).
2. For information on software image upgrade, see [Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller](#), on page 409.
3. Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.
Click the menu icon (☰) and choose **System Settings > Software Updates > Installed Apps**.
4. Integrate Cisco Identity Services Engine with Cisco DNA Center. After integration, any devices that Cisco DNA Center discovers along with relevant configurations and data are pushed to Cisco ISE.
5. Discover the Cisco Catalyst 9800 Series Wireless Controller.
You must enable NETCONF and set the port to 830 to discover the Cisco Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.
For more information, see [Discover Your Network Using CDP](#), on page 46 or [Discover Your Network Using an IP Address Range or CIDR](#), on page 48.
You must add the wireless management IP address manually.



Note On the Cisco Catalyst 9800 Series Wireless Controller, you must configure a static IP address for the wireless management interface to prevent provisioning failure.

While performing discovery using the Cisco Discovery Protocol (CDP) or an IP address range in the **Discovery** window, choose **Use Loopback** from the **Preferred Management IP** drop-down list to specify the device's loopback interface IP address.

6. Make sure that the discovered devices are displayed in the **Device Inventory** window and are in the **Managed** state.
For more information, see [About Inventory](#), on page 56 and [Display Information About Your Inventory](#), on page 57.
You must wait for the devices to move to a **Managed** state.
7. To verify the Assurance connection with the Cisco Catalyst 9800 Series Wireless Controller, use the following commands:

- **#show crypto pki trustpoints | sec DNAC-CA**

```
Trustpoint DNAC-CA
  Subject Name:
    cn=kube-ca
    Serial Number (hex): 00E*****
  Certificate configured.
```

- **#show crypto pki trustpoints | sec sdn-network**

```
Trustpoint sdn-network-infra-iwan:
```

```
Subject Name:
cn=sdn-network-infra-ca
  Serial Number (hex): 378*****
Certificate configured.
```

• **#show telemetry ietf subscription all**

```
Telemetry subscription brief
```

ID	Type	State	Filter type
1011	Configured	Valid	tdl-uri
1012	Configured	Valid	tdl-uri
1013	Configured	Valid	tdl-uri

• **#show telemetry internal connection**

```
Telemetry connection
```

Address	Port	Transport	State	Profile
IP address	25103	tls-native	Active	sdn-network-infra-iwan

• **#show network-assurance summary**

```
Network-Assurance           : True
Server Url                   : https://10.***.***.***
ICap Server Port Number     : 3***
Sensor Backhaul SSID        :
Authentication                : Unknown
```

8. Configure a TACACS server while configuring authentication and policy servers.

Configuring TACACS is not mandatory if you have configured the username locally on the Cisco Catalyst 9800 Series Wireless Controller.

9. Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center.

To import and upload an existing network hierarchy, see [Import Your Site Hierarchy to Cisco DNA Center, on page 128](#).

To create a new network hierarchy, see [Create, Edit and Delete a Site, on page 134](#) and [Add, Edit, and Delete a Building, on page 135](#).

10. Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

For more information, see [Work with APs on a Floor Map, on page 146](#).

11. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

For more information, see [Network Settings Overview, on page 191](#), [Configure Global Network Servers, on page 193](#), and [Add Cisco ISE or Other AAA Servers](#).

12. Create a wireless radio frequency profile with the parent profile as custom.

For more information, see [Create a Wireless Radio Frequency Profile, on page 227](#).

13. Create IP address pools at the global level.

Cisco DNA Center uses IP address pools to automate the configuration and deployment of SD-Access networks.

To create an IP address pool, see [Configure IP Address Pools, on page 202](#).

You must reserve an IP address pool for the building that you are provisioning. For more information, see [Provision a Network Through LAN Automation](#).

14. Create enterprise and guest wireless networks. Define the global wireless settings once; Cisco DNA Center then pushes the configurations to various devices across geographical locations.

Designing a wireless network is a two-step process. First, you must create SSIDs, and then associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

For more information, see [Create SSIDs for an Enterprise Wireless Network, on page 207](#) and [Create SSIDs for a Guest Wireless Network, on page 216](#). For information about other wireless settings, see [Configure Global Wireless Settings, on page 207](#).

15. Configure the backhaul settings. For more information, see [Manage Backhaul Settings, on page 265](#).

16. Configure the following in the **Policy** window for the Cisco Catalyst 9800 Series Wireless Controller:

- Create a virtual network. The virtual network segments your physical network into multiple logical networks.
- Create a group-based access control policy and add a contract. For more information, see [Create Group-Based Access Control Policy, on page 565](#).

17. Configure high availability.

For more information, see [Configure High Availability for the Cisco Catalyst 9800 Series Wireless Controller, on page 410](#).

18. Provision the Cisco Catalyst 9800 Series Wireless Controller with the configurations added during the design phase.

For more information, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).

19. Configure and deploy application policies on the Cisco Catalyst 9800 Series Wireless Controller.

For more information, see [Create an Application Policy, on page 602](#), [Deploy an Application Policy, on page 607](#), and [Edit an Application Policy, on page 606](#).



Note You must provision Cisco Catalyst 9800 Series Wireless Controller devices before deploying an application policy.

For Cisco Catalyst 9800 Series Wireless Controller devices, two different policies with different business relevance for two different SSIDs do not work. The last deployed policy always takes precedence when you are setting up relevance.

For Cisco Catalyst 9800 Series Wireless Controller devices, changing the default business relevance for an application does not work in FlexConnect mode.

You can apply an application policy only on a nonfabric SSID.

Software Image Upgrade Support for Cisco Catalyst 9800 Series Wireless Controller

Before you begin

- Discover the Cisco Catalyst 9800 Series Wireless Controller.

Enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Series Wireless Controller. NETCONF enables wireless services on the controller and provides a mechanism to install, manipulate, and delete the configuration of network devices.

For more information, see [Discover Your Network Using CDP, on page 46](#), or [Discover Your Network Using an IP Address Range or CIDR, on page 48](#).

- Make sure that the devices appear in the device inventory and are in the **Managed** state.

For more information, see [About Inventory, on page 56](#) and [Display Information About Your Inventory, on page 57](#).

-
- Step 1** Click the menu icon (☰) and choose **Design > Image Repository**.
The **Inventory** window is displayed with the discovered devices listed.
- Step 2** Import the Cisco Catalyst 9800 Series Wireless Controller software image from your local computer or from a URL.
For more information, see [Import a Software Image, on page 335](#).
- Step 3** Assign the software image to a device family.
For more information, see [Assign a Software Image to a Device Family, on page 336](#).
- Step 4** You can mark a software image as Golden by clicking the star for a device family or a particular device role.
For more information, see [Specify a Golden Software Image, on page 338](#).
- Step 5** Provision the software image.
Click the menu icon (☰) and choose **Provision > Device > Inventory**.
- Step 6** In the **Inventory** window, check the check box next to the Cisco Catalyst 9800 Series Wireless Controller whose image you want to upgrade.
- Step 7** From the **Actions** drop-down list, choose **Software Image > Image Update**.
For more information, see [Provision a Software Image, on page 341](#).
-

Configure High Availability for the Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Configuring High Availability (HA) on the Cisco Catalyst 9800 Series Wireless Controller involves the following prerequisites:

- Both the Cisco Catalyst 9800 Series Wireless Controller devices are running the same software version and have the active software image on the primary Catalyst 9800 Series Wireless Controller.
- The service port and management port of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured.
- The redundancy port of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are physically connected.
- Preconfigurations such as interface configurations, route addition, ssh line configurations, netconf-yang configurations are completed on the Catalyst 9800 Series Wireless Controller appliance.
- The management interface of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are in the same subnet.
- The discovery and inventory of Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 devices are successful from Cisco DNA Center.
- The devices are reachable and are in the **Managed** state.

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window is displayed with the discovered devices listed.

Step 2 To view devices available in a particular site, expand the **Global** site in the left pane, and select the site, building, or floor that you are interested in.

All the devices available in that selected site are displayed in the **Inventory** window.

Step 3 From the **Device Type** list, click the **WLCs** tab, and from the **Reachability** list, click the **Reachable** tab to get the list of wireless controllers that are discovered and reachable.

Step 4 In the **Inventory** window, click the desired Cisco Catalyst 9800 Series Wireless Controller name to configure as a primary controller.

Step 5 Click the **High Availability** tab.

The selected Catalyst 9800 Series Wireless Controller by default becomes the primary controller and the **Primary C9800** field is grayed out.

Step 6 From the **Select Primary Interface** and **Secondary Interface** drop-down lists, choose the interface that is used for HA connectivity.

The HA interface serves the following purposes:

- Enables communication between the controller pair before the IOSd boots up.
- Provides transport for IPC across the controller pair.

- Enables redundancy across control messages exchanged between the controller pair. The control messages can be HA role resolution, keepalives, notifications, HA statistics, and so on.

Step 7 From the **Select Secondary C9800** drop-down list, choose the secondary controller to create an HA pair.

Note When you choose the secondary controller, based on the wireless management interface IP subnet of the primary controller, the redundancy management IP is auto populated, and an **i** icon is displayed at the top of the **High Availability** window, along with the following message:

Ensure that the Redundancy Management IP and Peer Redundancy Management IP are not assigned to any other network entities. If the IPs are in use, change the IPs accordingly and configure.

Step 8 Enter the **Redundancy Management IP** and **Peer Redundancy Management IP** addresses in the respective fields.

Note

- The IP addresses used for the redundancy management IP and peer redundancy management IP should be configured in the same subnet as the management interface of the Cisco Catalyst 9800 Series Wireless Controller. Ensure that these IP addresses are unused IP addresses within the subnet range.
- Cisco DNA Center only pushes the management IP address of the Cisco Catalyst 9800 Series Wireless Controller to the Cisco ISE network access device list. Whereas the standby controller uses the redundancy management IP address to initiate AAA requests. So, you must add the redundancy management IP addresses to the AAA servers for a seamless client authentication and standby monitoring.

Step 9 In the **Netmask** field, enter the netmask address.

Step 10 Click **Configure HA**.

The HA configuration is initiated at the background using the CLI commands. First, the primary controller is configured. On success, the secondary controller is configured. Both the devices reboot once the HA is enabled. This process may take up to 2.5 minutes to complete.

Step 11 After the HA is initiated, the **Redundancy Summary** under **High Availability** tab displays the **Sync Status** as **HA Pairing is in Progress**. When Cisco DNA Center finds that the HA pairing is successful, the **SyncStatus** becomes **Complete**.

This is triggered by the inventory poller or manual resynchronization. By now, the secondary controller (Catalyst 9800 Series Wireless Controller 2) is deleted from Cisco DNA Center. This flow indicates successful HA configuration in the Catalyst 9800 Series Wireless Controller.

Step 12 To manually resynchronize the controller, on the **Provision > Inventory** window, select the controller that you want to synchronize manually.

Step 13 From the **Actions** drop-down list, choose **Resync**.

Step 14 The following is the list of actions that occur after the process is complete:

- Catalyst 9800 Series Wireless Controller 1 and Catalyst 9800 Series Wireless Controller 2 are configured with redundancy management, redundancy units, and Single sign-on (SSO). The devices reboot in order to negotiate their role as an active controller or a standby controller. The configuration is synchronized from active to standby.

Note If you've configured a AAA server or Cisco ISE server for client and endpoint authentication in Cisco DNA Center then in a HA setup, the CTS credentials for active and standby controllers are synchronized and hence, during a HA switchover, Cisco DNA Center does not update the CTS credentials for the wireless controllers on Cisco ISE.

- On the **Show Redundancy Summary** window, you can see these configurations:
 - SSO is enabled.
 - The Catalyst 9800 Series Wireless Controller 1 is in the active state.
 - The Catalyst 9800 Series Wireless Controller 2 is in the standby state.

Information About High Availability

High Availability (HA) allows you to reduce the downtime of wireless networks that occurs because of the failover of controllers. You can configure HA on Cisco Catalyst 9800 Series Wireless Controller through Cisco DNA Center.

Commands to Configure High Availability on Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Use the following commands to configure HA on the primary controller for Cisco Catalyst 9800 Series Wireless Controller:

- Run the **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

This example shows how to configure an HA chassis interface:

```
chassis ha-interface GigabitEthernet 3 local-ip 192.0.2.2 255.255.255.0
remote-ip 192.0.2.3
```

- Run the **reload** command to reload devices for the changes to become effective.

Step 2 Use the following commands to configure HA on the secondary controller for Catalyst 9800 Series Wireless Controller:

- Run the **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

This example shows how to configure an HA chassis interface:

```
chassis ha-interface GigabitEthernet 2 local-ip 192.0.2.3 255.255.255.0
remote-ip 192.0.2.2
```

Step 3 Run the **chassis clear** command to clear or delete all the HA-related parameters, such as the local IP, remote IP, HA interface, mask, timeout, and priority.

Note Reload the devices for changes to take effect by running the **reload** command.

Step 4 Use the following commands to configure HA on the primary controller for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the **chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

This example shows how to configure an HA chassis interface:

```
chassis ha-interface local-ip 192.0.2.2 255.255.255.0 remote-ip 192.0.2.3
```

- Run the **reload** command to reload devices for the changes to become effective.

Step 5 Use the following commands to configure HA on the secondary controller for Cisco Catalyst 9800-40 Wireless Controller and Cisco Catalyst 9800-80 Wireless Controller devices:

- Run the **chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** command to configure the HA chassis interface.

This example shows how to configure an HA chassis interface:

```
chassis ha-interface local-ip 192.0.2.3 255.255.255.0 remote-ip 192.0.2.2
```

Step 6 Run the **chassis clear** command to clear or delete all the HA-related parameters, such as the local IP, remote IP, HA interface, mask, timeout, and priority.

Note Reload the devices for changes to take effect by running the **reload** command.

Commands to Verify Cisco Catalyst 9800 Series Wireless Controllers High Availability

Use the following commands to verify the high availability configurations from Cisco Catalyst 9800 Series Wireless Controller:

- Run the **config redundancy mode sso** command to check the HA-related details.
- Run the **show chassis** command to view chassis configurations about the HA pair, including the MAC address, role, switch priority, and current state of each controller device in the redundant HA pair.
- Run the **show ip interface brief** command to view the actual operating redundancy mode running on the device, and not the configured mode as set by the platform.
- Run the **show redundancy states** command to view the redundancy states of the active and standby controllers.
- Run the **show redundancy summary** command to check the configured interfaces.
- Run the **show romvar** command to verify high availability configuration details.

N+1 High Availability

Overview of N+1 High Availability

Cisco DNA Center supports N+1 High Availability (HA) on Cisco AireOS wireless controllers and Cisco Catalyst 9800 Series Wireless Controllers.

Cisco AireOS wireless controllers have a dedicated stock-keeping unit (SKU) for their N+1 controllers. Cisco Catalyst 9800 Series Wireless Controllers don't have a dedicated SKU; the same model must be used for HA.

The N+1 HA architecture provides redundancy for controllers across geographically separated data centers with low-cost deployments.

N+1 HA allows Cisco Wireless Controllers to be used as backup controllers for multiple primary controllers. These wireless controllers are independent of each other and do not share configuration or IP addresses on

any of their interfaces. When a primary wireless controller resumes operation, the APs fall back automatically from the backup wireless controller to the primary wireless controller if the AP fallback option is enabled.

Cisco DNA Center supports primary and secondary controller configurations for N+1 HA.

N+1 HA is configured at the AP level, not at the global level. Configurations are pushed directly to the AP.



Note The primary and secondary controllers must be of the same device type. For example, if the primary device is a Catalyst 9800 Series Wireless Controller, the secondary device must also be a Catalyst 9800 Series Wireless Controller.

APs with higher priority on the primary controller always connect first to the backup controller, even if they have to push out the lower priority APs.

The N+1 HA configuration has the following limitations:

- Auto provisioning of a secondary controller is not supported because of the VLAN ID configuration.
- You must reprovision the secondary controller manually with the latest design configuration if you made any changes to the primary controller.
- Cisco DNA Center does not support fault tolerance.
- Access Point Stateful Switch Over (AP SSO) functionality is not supported for N+1 HA. The AP Control and Provisioning of Wireless Access Points (CAPWAP) state machine is restarted when the primary controller fails.

Prerequisites for Configuring N+1 High Availability from Cisco DNA Center

- Discover primary and the secondary controller by running the Discovery feature.

For more information, see [Discover Your Network Using CDP, on page 46](#), or [Discover Your Network Using an IP Address Range or CIDR, on page 48](#).

- Make sure that the wireless controllers are reachable and in the Managed state.

For more information, see [About Inventory, on page 56](#) and [Display Information About Your Inventory, on page 57](#).

- Verify the network connectivity between devices. If the primary controller goes down, the AP should be able to join the secondary controller through the N+1 configuration.
- Create two buildings to manage the primary and secondary locations for both devices. For example, create two buildings, *Building A* and *Building B*, where Building A is the primary managed location for controller-1 and also the secondary managed location for controller-2, and Building B is configured only as a primary managed location for controller-2.

For more information, see [Create, Edit and Delete a Site, on page 134](#) and [Add, Edit, and Delete a Building, on page 135](#).

- Add and position APs on a floor map to get a coverage heatmap visualization during the design phase.

For more information, see [Work with APs on a Floor Map, on page 146](#).

- Create two SSIDs and associate them as the backhaul SSIDs.

For more information, see [Create SSIDs for an Enterprise Wireless Network, on page 207](#) and [Create SSIDs for a Guest Wireless Network, on page 216](#).

Configure N+1 High Availability from Cisco DNA Center

This procedure shows how to configure N+1 High Availability (HA) on Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window is displayed with the discovered devices listed.
- Step 2** Check the check box next to the desired controller to provision it as a primary controller.
- Step 3** From the **Actions** drop-down list, choose **Provision > Provision Device**.
The **Assign Site** window is displayed.
- Step 4** Click **Choose a site** to assign a primary managed AP location for the primary controller.
- Step 5** In the **Choose a site** window, select a site and click **Save**.
- Step 6** Click **Next**.
The **Configuration** window is displayed, which shows the primary AP managed location for the primary device.
- Step 7** Add or update the managed AP locations for the primary controller by clicking **Select Primary Managed AP Locations**.
- Step 8** In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.
You can either select a parent site or the individual sites.
- Step 9** Configure the interface and VLAN details.
- Step 10** Under **Configure Interface and VLAN** area, configure the IP address and subnet mask details, and click **Next**.
- Step 11** In the **Advanced Configuration** window, configure values for the predefined template variables, and click **Next**.
- Step 12** In the **Summary** window, verify the managed AP locations for the primary controller and other configuration details, and click **Deploy**.
- Step 13** Click **Now** to deploy the device immediately. Click **Later** to schedule the deployment for a later time.
- Step 14** To provision the secondary controller, in the **Inventory** window, check the check box next to the desired controller to provision it as a secondary controller.
- Step 15** From the **Actions** drop-down list, choose **Provision > Provision Device**.
The **Assign Site** window is displayed.
- Step 16** Click **Choose a site** to assign the managed AP location for the secondary controller.
The managed AP location for the secondary controller should be same as the managed AP location of the primary controller.
- Step 17** In the **Choose a site** window, check the check box next to the site name to associate the secondary controller, and click **Save**.
- Step 18** Click **Next**.
The **Configuration** window is displayed, which shows the primary AP managed and secondary AP managed locations for the secondary device.

- Step 19** Add or update the managed AP locations for the secondary controller by clicking **Select Secondary Managed AP Locations**.
- Step 20** In the **Managed AP Location** window, check the check box next to the site name, and click **Save**.
You can either select a parent site or the individual sites.
- Step 21** Configure the interface and VLAN details for the secondary controller.
- Step 22** Under the **Configure Interface and VLAN** area, configure the IP address and subnet mask details for the secondary controller, and click **Next**.
- Step 23** In the **Advanced Configuration** window, configure values for the predefined template variables, and click **Next**.
- Step 24** In the **Summary** window, verify the managed AP locations for the secondary controller and other configuration details, and click **Deploy**.
- Step 25** Click **Now** to deploy the device immediately. Click **Later** to schedule the deployment for a later time.
- Step 26** To verify the managed locations of the primary and secondary controllers, click the device name of the controllers that you provisioned on the **Provision > Network Devices > Inventory** window.
- Step 27** In the dialog box, click **View Device Details**.
- Step 28** In the device details window, click the **Managed ap locations** tab to view the primary and secondary managed location details.
- Step 29** Provision the AP for the primary controller.
- Step 30** On the **Network Devices > Inventory** window, check the check box next to the AP that you want to provision.
- Step 31** From the **Actions** drop-down list, choose **Provision > Provision Device**.
- Step 32** In the **Assign Site** window, click **Choose a Floor** to select the floor from the primary managed location.
- Step 33** Click **Next**.
The **Configuration** window is displayed.
- Step 34** By default, the custom RF profile that you marked as the default under **Design > Network Settings > Wireless > Wireless Radio Frequency Profile** is chosen in the **RF Profile** drop-down list.
You can change the default RF Profile value for an AP by selecting a value from the **RF Profile** drop-down list.
- Step 35** Click **Next**.
- Step 36** In the **Summary** window, review the configuration details.
- Step 37** Click **Deploy** to provision the primary AP.
- Step 38** You are prompted with a message that creation or modification of an AP group is in progress.
You are prompted with a message stating `After provisioning AP(s) will reboot. Do you want to continue?`.
- Step 39** Click **OK**.
When deployment succeeds, the **Last Sync Status** column in the **Device Inventory** window shows **SUCCESS**.
-

Mobility Configuration Overview

The mobility configuration in Cisco DNA Center allows you to group a set of Cisco Wireless Controllers into a mobility group for a seamless roaming experience of wireless clients.

By creating a mobility group, you can enable multiple wireless controllers in a network to dynamically share information and forward traffic when inter-controller or inter-subnet roaming occurs. 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 wireless controllers within the same wireless network.

Cisco DNA Center allows you to create mobility groups between various platforms, such as Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

The mobility configuration has the following guidelines and limitations:

- You cannot select multiple controllers for configuring mobility on the **Provision** window.
- You cannot create mobility groups with the group name as default. This resets the mobility and RF group names as default and deletes all the peers.
- You cannot configure a mobility group name on the anchor controller.
- You must reboot the wireless controller manually if there is a change to the virtual IP address when configuring mobility groups on Cisco AireOS Controllers.
- Wireless controllers with the same mobility group name are automatically grouped into a single mobility group and added as peers to each other.
- When configuring mobility groups on Cisco AireOS Controllers, if the wireless controllers do not have the IP address 192.0.2.1, Cisco DNA Center pushes the virtual IP address 192.0.2.1 to all the wireless controllers.
- Do not explicitly add guest anchor controllers to the mobility group. The provisioned guest anchor controllers do not appear in the drop-down list while adding peers in the mobility configuration window.
- If you provision a wireless controller as a guest anchor, ensure that it is not added to the mobility group.

Mobility Configuration Workflow

Here is the workflow that you can follow to configure mobility on Cisco Wireless Controller:

- To configure mobility, you must provision a wireless controller with the mobility group name, RF group name, and mobility peers.
- The configuration that is applied during the wireless controller provisioning is automatically replicated to all the mobility peers configured in that group.
- Resynchronize the wireless controllers to get the latest tunnel status.

Mobility Configuration Use Cases

The following use cases explain the steps to configure mobility between controllers.

Use Case 1

This use case assumes that wireless controller 1, wireless controller 2, and wireless controller 3 are newly added to Cisco DNA Center with the mobility group name, "Default." These wireless controllers aren't yet provisioned.

1. Provision wireless controller 1 by configuring the mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.

2. Provision wireless controller 2.

In the **Provision** window, the mobility configuration is automatically populated for wireless controller 2 with the group name and peers.

3. Provision wireless controller 3.

4. After provisioning all the wireless controllers, resynchronize the wireless controllers to receive the latest tunnel status.

Use Case 2

This use case assumes that wireless controller 1, wireless controller 2, and wireless controller 3 have already been added to Cisco DNA Center with different mobility group names. These wireless controllers are provisioned.

1. Provision wireless controller 1 by configuring the mobility group name, RF group name, and adding wireless controller 2 and wireless controller 3 as peers.
2. The mobility configuration is automatically replicated across other peers, such as wireless controller 2 and wireless controller 3.
 - After the successful provisioning of wireless controller 1, wireless controller 2 and wireless controller 3 are added as peers on the wireless controller 1.
 - On wireless controller 2, wireless controller 1 and wireless controller 3 are added as peers.
 - On wireless controller 3, wireless controller 1 and wireless controller 2 are added as peers.

Configure Mobility Group

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window is displayed, which lists all the discovered devices.

Step 2 Check the check box next to the Cisco Catalyst 9800 Series Wireless Controller name for which you want to configure mobility.

Step 3 From the **Actions** drop-down list, choose **Provision > Configure WLC Mobility**.

The **Configure Mobility Group** slide-in pane is displayed.

For more information, see [Mobility Configuration Overview, on page 416](#).

Step 4 From the **Mobility Group Name** drop-down list, you can either add a new mobility group by clicking +, or choose from the existing mobility groups.

Information about the existing mobility peers is loaded from the intent available in Cisco DNA Center.

Note If you choose the default mobility group from the drop-down list, you cannot add mobility peers.

Step 5 In the **RF Group Name** field, enter a name for the RF group.

Step 6 To enable Datagram Transport Layer Security (DTLS) data encryption, click the **Data Link Encryption** button on.

Step 7 To enable or disable Cipher configuration for mobility, use the **DTLS High Cipher Only** toggle button.

Cipher configuration is applicable for Cisco Catalyst 9800 Series Wireless Controller Release 17.5 or later. You must manually reboot the device for changes to take effect.

- Step 8** To manually reboot the device after making changes in the DTLS cipher configuration to take effect after provision, enable the **Restart for DTLS Ciphers to take effect** toggle button.
- Step 9** Under **Mobility Peers**, click **Add** to configure a mobility peer.
- Step 10** In the **Add Mobility Peer** slide-in pane, configure the following:
- a) Choose one of the following types of mobility peers:
 - To include mobility peers that are managed by Cisco DNA Center, click **Managed WLC**.
 - To include mobility peers that are not managed by Cisco DNA Center, click **External WLC**.
 - b) If you choose **Managed WLC**, from the **Device Name** drop-down list, choose the controller.

After the device is provisioned, Cisco DNA Center creates a mobility group in the device, assigns the RF group, and configures all ends of peers. The mobility group configuration is deployed automatically to all the selected peer devices.
 - c) If you choose **External WLC**, configure the following:
 - In the **Device Name** field, enter the device name.
 - (Optional) From the **Device Series** drop-down list, choose the device series.
 - In the **Public IP Address** field, enter the public IP address.
 - (Optional) In the **Private IP Address** field, enter the private IP address.
 - In the **MAC Address** field, enter the MAC address of the device.
 - In the **Mobility Group Name** field, enter the mobility group name.
 - (Optional) In the **Hash** field, enter the hash for the Cisco Catalyst 9800 Series Wireless Controller.

Note This field is available only for Cisco Catalyst 9800-CL Wireless Controller.
 - d) Click **Save**.

Step 11 Click **Configure Mobility**.

Step 12 You can reset the mobility group name and the RF group name using one of the following methods:

- In the **Configure Mobility Group** slide-in pane, choose **default** from the **Mobility Group Name** drop-down list.
- In the **Configure Mobility Group** slide-in pane, click **Reset Mobility**.

This step automatically sets the **RF Group Name** to **default** and removes all peers. After you provision, the mobility on the device is set and the device is removed from all other peers.

About DTLS Ciphersuites

Ciphersuites are a set of encryption and integrity algorithms designed to protect radio communication on your wireless LAN.

You can configure multiple DTLS (Data Datagram Transport Layer Security) Ciphersuites on Cisco Catalyst 9800 Series Wireless Controller, Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches, and Cisco Embedded Wireless Controller on Catalyst Access Points platforms running Release 17.5 or later.

Configure Multiple DTLS Ciphersuites

You can configure DTLS Ciphersuites either at the global level or site level.

Before you begin

- Make sure that the Device Controllability feature is enabled on the **System > Settings > Device Settings > Device Controllability** window.
- Discover Cisco Catalyst 9800 Series Wireless Controllers in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.

-
- Step 1** Click the menu icon (☰) and choose **Design > Network Settings > Wireless**.
- Step 2** From the left hierarchy tree, choose **Global** to configure all sites with the same DTLS Ciphersuite configuration.
From the left hierarchy tree, choose a site to configure DTLS Ciphersuites at the site level. The DTLS Ciphersuite configuration will be pushed to the controller available on that particular site.
- Step 3** Uncheck the **Skip DTLS Ciphersuite Config** check box to configure Ciphersuites as part of Device Controllability.
- Step 4** Configure either default Ciphersuites or custom Ciphersuites.
By default, the **Default** Ciphersuite is selected.
The Default Ciphersuite box shows the list of default Ciphersuites and these Ciphersuites are configured as default on the device. You cannot change the priority of these default ciphersuites.
- Step 5** To configure custom Ciphersuites, click the **Custom** button.
Custom Ciphersuite overrides the default Ciphersuites with priority.
- Step 6** From the **Version** drop-down list, choose the DTLS version.
Based on the DTLS version, Cisco DNA Center shows the available Ciphersuites.
- Step 7** Click the blue button next to the Ciphersuite if you do not want to apply any of the Ciphersuites.
- Step 8** To change the priority of Ciphersuites, drag each Ciphersuite.
- Step 9** Click **Save**.
The message `DTLS Ciphersuite Config Saved successfully` is displayed.
- Step 10** To apply the Ciphersuite configuration, you must provision the device.
For more information, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).
-

About N+1 Rolling AP Upgrade

The Rolling AP Upgrade feature is supported on the Cisco Catalyst 9800 Series Wireless Controller in an N+1 High Availability setup. This feature helps you upgrade software images on the APs associated with the Cisco Catalyst 9800 Series Wireless Controller in your wireless LAN network. To achieve the zero downtime, it is possible to upgrade APs in a staggered way using the N+1 Rolling AP Upgrade feature.

The primary controller identifies the candidate APs through the radio resource management neighbor AP map. The upgrade process starts with the software image downloading to the primary controller while the image is predownloaded to the candidate APs. After the candidate APs have been upgraded and rebooted, they join the secondary controller in a staggered manner. After all the APs have joined the secondary controller, the primary controller reboots. The APs rejoin the primary controller in a staggered manner after it is rebooted.

Here are the prerequisites for configuring the Rolling AP Upgrade feature:

- An N+1 High Availability setup with two wireless controllers, one as the primary controller and the other one as the secondary.
- The primary and the N+1 controllers have the same configuration and manage the same location in the network.
- The N+1 controller is already running the Golden image so that Rolling AP Upgrade works with zero downtime.

Golden images are standardized images for network devices and Cisco DNA Center automatically downloads the images from Cisco.com. Image standardization helps in device security and optimal device performance.

- The N+1 controller is reachable and in **Managed** state in Cisco DNA Center.
- Both the controllers are part of the same mobility group, and a mobility tunnel is established between the primary and N+1 controller. The upgrade information between the primary and N+1 controllers are exchanged through the mobility tunnel.



Note If you have a cyclic N+1 HA deployment, where *wireless controller 1* is N+1 for *wireless controller 2* and *wireless controller 2* is N+1 for *wireless controller 1*, you cannot perform a rolling AP upgrade on both devices. Instead, one controller must go through a normal upgrade. You can perform a rolling AP upgrade on the other controller after the first controller is upgraded without the rolling AP upgrade.

Workflow to Configure a Rolling AP Upgrade

This procedure shows how to configure a Rolling AP Upgrade on Cisco Catalyst 9800 Series Wireless Controllers.



Note N+1 Rolling AP Upgrade is supported on fabric and nonfabric deployments.

Step 1

Install Cisco DNA Center.

For more information, see the [Cisco Digital Network Architecture Center Installation Guide](#).

- Step 2** Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.
Click the menu icon (☰) and choose **System > Software Updates > Installed Apps**.
- Step 3** Discover the wireless controller using the Discovery feature.
You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete the configurations on network devices.
For more information, see [Discover Your Network Using CDP, on page 46](#) or [Discover Your Network Using an IP Address Range or CIDR, on page 48](#).
- Step 4** Make sure that the discovered devices appear in the **Device Inventory** window and are in the **Managed** state.
For more information, see [About Inventory, on page 56](#) and [Display Information About Your Inventory, on page 57](#).
You must wait for devices to move to a **Managed** state.
- Step 5** Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.
You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center.
To import and upload an existing network hierarchy, see [Import Your Site Hierarchy to Cisco DNA Center, on page 128](#).
To create a new network hierarchy, see [Create, Edit and Delete a Site, on page 134](#) and [Add, Edit, and Delete a Building, on page 135](#).
- Step 6** Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.
For more information, see [Work with APs on a Floor Map, on page 146](#).
- Step 7** Provision the primary controller with the primary managed AP location, Rolling AP Upgrade enabled, and mobility group configured with the secondary controller as its peer.
To do this, choose **Provision > Network Devices > Inventory**, and check the check box next to the primary controller name.
- Step 8** Configure the N+1 controller as the mobility peer in the Mobility Group configuration.
For more information, see [Mobility Configuration Overview, on page 416](#).
- Step 9** Provision the N+1 HA controller by configuring the primary controller's primary managed AP location as the N+1 controller's secondary managed AP location. This configures the secondary controller as the N+1 controller.
For more information, see [Provision a Cisco Catalyst 9800 Series Wireless Controller, on page 423](#).
- Step 10** Provision the APs that are associated with the primary controller.
- Step 11** Import the software images to the repository.
For more information, see [Import a Software Image, on page 335](#).
- Step 12** Assign the software image to a device family.
For more information, see [Assign a Software Image to a Device Family, on page 336](#).
- Step 13** Mark the software image as Golden by clicking the star for a device family or a device role.
For more information, see [Specify a Golden Software Image, on page 338](#).

- Step 14** Before upgrading the image, make sure that the image readiness checks are successful for both devices. Also make sure that the status of the **N+1 Device Check** and the **Mobility Tunnel Check** has a green tick mark.
- To do the image update readiness check, choose **Provision > Network Devices > Software Images**.
 - From the **Focus** drop-down list, choose **Software Images**. Select the device whose image you want to upgrade.
 - If the prechecks are successful for a device, the **Status** link in the **Image Precheck Status** column has a green tick mark. If any of the upgrade readiness prechecks fail for a device, the Image Precheck Status link has a red mark, and you cannot update the OS image for that device. Click the **Status** link and correct any errors before proceeding.
- Step 15** Initiate the upgrade on primary controller.
- Step 16** On the **Software Images** window, check the check box next to the primary controller.
- Step 17** From the **Actions** drop-down list, choose **Software Image > Update Image**.
For more information, see [Provision a Software Image, on page 341](#).
- Step 18** To monitor the progress of the image upgrade, click **In Progress** in the **Software Image** column. The **Device Status** window displays the following information:
- **Distribution Operation:** Provides information about the image distribution process. The image gets copied from Cisco DNA Center to the primary device. The activate operation starts after the distribution process is complete.
 - **Activate Operation:** Provides the activate operation details. The Rolling AP Upgrade starts during this process.
 - **Rolling AP Upgrade Operation:** Provides a summary of the Rolling AP Upgrade, such as whether the Rolling AP Upgrade task is complete, the number of APs pending, the number of rebooting APs, and the number of APs that have joined the N+1 controller.
- Click **View AP Status** to view details about the primary controller, N+1 controller, device names, current status, and iterations.
-

Provision a Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Before provisioning a Cisco Catalyst 9800 Series Wireless Controller make sure that you have completed the steps in [Configure a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center, on page 406](#).

- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window is displayed, which lists all the discovered devices.
- Step 2** Check the check box next to the Catalyst 9800 Series Wireless Controller name that you want to provision.
- Step 3** From the **Actions** drop-down list, choose **Provision > Provision Device**.
- Step 4** In the **Assign Site** window, click **Choose a Site** to associate with a site.
- Step 5** In the **Choose a site** slide-in pane, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller, and click **Save**.

You can either select a parent site or the individual sites. If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect an individual site.

Step 6 Click **Next**.

The **Configuration** window is displayed.

Step 7 Select a role for the Cisco Catalyst 9800 Series Wireless Controller: **Active Main WLC** or **Anchor**.

Step 8 Click **Select Primary Managed AP Locations** to select the managed AP location for the primary controller.

Step 9 Click **Select Secondary Managed AP Locations** to select the managed AP location for the secondary controller.

Step 10 You can either select a parent site or the individual sites, and click **Save**.

If you select a parent site, all the children under the parent site are also selected. You can uncheck the check box to deselect a particular site.

Note The inheritance of managed AP locations allows you to automatically choose a site along with the buildings and floors under that particular site. One site is managed by only one wireless controller.

Step 11 (Optional) Check the **AP Authorization List** check box to choose the authorization list for AP authorization, and do the following:

Note This check box is displayed only if an AP authorization list is available. For more information about AP authorization list, see [Create an AP Authorization List, on page 250](#).

- From the **AP Authorization List Name** drop-down list, choose an AP authorization list. Based on the content of the AP authorization list, Cisco DNA Center displays a message indicating the corresponding primary authorization type and failback mechanism.
- (Optional) To view the entries for the selected AP authorization list, click **View Entries**.
- If the wireless controller manages both mesh and nonmesh APs, Cisco DNA Center displays the **Authorize Only Mesh Access Points** and **Authorize All Access Points** check boxes.

To enable authorization for only mesh APs, check the **Authorize Only Mesh Access Points** check box.

To enable authorization for all APs, check the **Authorize All Access Points** check box.

Step 12 For an active main wireless controller, you need to configure interface and VLAN details.

Step 13 Under the **Assign Interface** area, do the following:

- **VLAN ID:** Enter a value for the VLAN ID.
- **Interface IP Address:** Enter a value for the interface IP address.
- **Gateway IP Address:** Enter the gateway IP address.
- **Subnet Mask (in bits):** Enter the subnet mask details for the interface.

Note Assigning an IP address, gateway IP address, and subnet mask is not required for the Cisco Catalyst 9800 Series Wireless Controller.

Step 14 Check the **Skip AP Provision** check box to skip configuring AP related commands while provisioning the Cisco Catalyst 9800 Series Wireless Controller.

Step 15 Click **Next**.

The **Model Configuration** window is displayed.

- Step 16** In the **Devices** pane, you can either search for a model config design by entering its name in the **Find** field, or expand the device and select a model configuration design.
- The selected model configuration design is displayed in the right pane.
- Step 17** Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the model configuration design. You cannot edit all the configurations at this step.
- Step 18** After making the necessary changes, click **Apply**.
- Step 19** Click **Next**.
- The **Advanced Configuration** window is displayed, which is where you enter values for the predefined template variables.
- Step 20** Search for the device or the template in the **Devices** panel.
- Step 21** Enter a value for the predefined template variable in the **wlanid** field, and click **Next**.
- Step 22** In the **Summary** window, review the configuration settings and click **Deploy**.
- Step 23** Click **Now** to deploy the device immediately. Click **Later** to schedule the deployment for a later time.
- Step 24** To verify the configurations that are pushed from Cisco DNA Center to the device, use the following commands on the Cisco Catalyst 9800 Series Wireless Controller device:
- #show wlan summary
 - #show run | sec line
 - #show running-configuration
- Step 25** After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.
- Step 26** In the **Inventory** window, click **See Details** in the **Provision Status** column against a device to get more information about network intent or to view a list of actions.
- Step 27** Click **See Details** under **Device Provisioning**.
- Step 28** Click **View Details** under **Deployment of network intent**, and click the device name.
- Step 29** Click and expand the device name.
- Step 30** Expand the **Configuration Summary** area to view the operation details, feature name, and management capability. The configuration summary also displays any error that occurred while provisioning the device with the reasons for failure.
- Step 31** Expand the **Provision Summary** area to view details of the exact configuration that is sent to the device.
- Step 32** Provision the AP.

Configure Cisco Wireless Controllers on the Existing Infrastructure

With Cisco DNA Center, you can add and provision devices such as Cisco Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers in the existing deployment.

Before you begin

- Start by running a Discovery job on the device. All your devices are displayed on the **Inventory** window. For more information, see [Discover Your Network, on page 37](#) and [About Inventory, on page 56](#).

- The wireless controller should be reachable and in Managed state on the **Inventory** window. For more information, see [About Inventory, on page 56](#).
- To discover Cisco Catalyst 9800 Series Wireless Controller, you must enable NETCONF and set the port to 830. For more information, see [Discovery Overview, on page 37](#).
- Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations. You can either create a new network hierarchy or, if you have an existing network hierarchy on Cisco Prime Infrastructure, import it into Cisco DNA Center. For more information about importing and uploading an existing network hierarchy, see [Import Your Site Hierarchy to Cisco DNA Center, on page 128](#).
For more information about creating a new network hierarchy, see [Create, Edit and Delete a Site, on page 134](#) and [Add, Edit, and Delete a Building, on page 135](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window is displayed with the discovered devices listed.
- Step 2** Click **Filter** and enter the appropriate values in the selected filter field. For example, for the **Device Name** filter, enter the name of the device.
The data that is displayed in the **Devices** table is automatically updated according to your filter selection.
- Step 3** Check the check box next to the wireless controller device name that you want to provision.
- Step 4** From the **Actions** drop-down list, choose **More > Learn Device Config**.
The **Site Assignment** window opens and the **Learn Device Configuration** workflow begins.
- Note** You can also start this workflow by doing the following:
- a. From the **Inventory** window, click the device's link to open a popup window that provides high-level information for that device.
 - b. Click **View Device Details** to open the device's details page.
 - c. Click **Learn WLC Config**.
- Step 5** Follow Step 3 through Step 13 in [Learn Device Configurations from Devices with Pre-Existing Infrastructure, on page 724](#).
- Step 6** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
- Step 7** Click **Filter** to locate the device that you want to provision.
The data that is displayed in the **Devices** table is automatically updated according to your filter selection.
- Step 8** Check the check box next to the wireless controller that you want to provision.
- Step 9** From the **Actions** drop-down list, choose **Provision > Provision Device**.
- Step 10** Review the details in the **Assign Site** step, and click **Next**.
- Step 11** In the **Configuration** step, configure the following:
- a) Under **Interface and VLAN Configuration**, click **+Add** to configure interface and VLAN details.
 - b) In the **Configure Interface and VLAN** window, configure the required fields, and click **OK**.
 - c) Click **Next**.

- Step 12** In the **Model Configuration** step, configure the following.
- In the **Devices** pane, you can either search for a model config design by entering its name in the Find field, or expand the device and select a model config design. The selected model config design is displayed in the right pane.
 - Check the check box next to the **Design Name** that you want to provision, and click **Configure** to edit the model config design. You cannot edit all the configurations at this step.
 - After making the necessary changes, click **Apply**.
 - Click **Next**.
- Step 13** In the **Advanced Configuration** window, you can enter values for the predefined template variables.
- Search for the device or the template in the Devices panel.
 - Enter a value for the predefined template variable in the **wlanid** field, and click **Next**.
- Step 14** In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)
- Step 15** To proceed, click **Deploy**.
- Step 16** In the **Schedule** window, click **Now** or **Later** to indicate when you want to start the configuration, and click **Apply**.
- Step 17** Provision the AP. For information, see [Provision a Cisco AP—Day 1 AP Provisioning, on page 397](#).
-

Day 0 Workflow for Cisco Embedded Wireless Controller on Catalyst Access Points

The Cisco Embedded Wireless Controller on Catalyst Access Points (EWC-APs) is the next-generation Wi-Fi solution, which combines the Cisco Catalyst 9800 Series Wireless Controller with Cisco Catalyst 9100 Series Access Points, creating the best-in-class wireless experience for the evolving and growing organization.

Before you begin

- Design your network hierarchy with sites, buildings, floors, and so on.
For more information, see [Create, Edit and Delete a Site, on page 134](#) and [Add, Edit, and Delete a Building, on page 135](#).
- Define the device credentials, such as CLI, SNMP, HTTP, and HTTPS at the global level. The credentials that are defined at the global level are inherited by the sites.
For more information, see [Configure Global CLI Credentials, on page 194](#), [Configure Global SNMPv2c Credentials, on page 195](#), and [Configure Global SNMPv3 Credentials, on page 195](#).
- Create wireless SSIDs, wireless interfaces, and wireless Radio Frequency profiles.
For more information, see [Create SSIDs for an Enterprise Wireless Network, on page 207](#), [Create SSIDs for a Guest Wireless Network, on page 216](#), [Create a Wireless Interface, on page 225](#), and [Create a Wireless Radio Frequency Profile, on page 227](#).



Note For Cisco Embedded Wireless Controller on Catalyst Access Points, only Flex-based SSID creation is supported.

- Configure the DHCP server with Option #43 on the switch where the Cisco Embedded Wireless Controller on Catalyst Access Points is connected. This is IP address of the Cisco DNA Center Plug and Play server. Using this IP address, the APs contact the PnP server and download the configuration.
- Make sure that you have the Cisco Embedded Wireless Controller on Catalyst Access Points in the inventory. If not, discover them using the Discovery feature. For more information, see [Discover Your Network Using CDP, on page 46](#), [Discover Your Network Using an IP Address Range or CIDR, on page 48](#), and [About Inventory, on page 56](#).
- The APs should be in the factory reset state without any Cisco Wireless Controller configurations.

The Cisco Embedded Wireless Controller on Catalyst Access Points is available in multiple form factors:

- Cisco Embedded Wireless Controller on Catalyst 9115AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9117AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9120AX Access Points
- Cisco Embedded Wireless Controller on Catalyst 9130AX Access Points

Step 1 The Cisco Embedded Wireless Controller on Catalyst Access Points contacts the DHCP server.

In response, the DHCP server provides the IP address along with Option #43, which contains the IP address of the Cisco Plug and Play server.

Step 2 Based on Option #43, the Cisco Embedded Wireless Controller on Catalyst Access Points turns on the Plug and Play agent and contacts the Cisco DNA Center Plug and Play server.

Note If you have a set of Cisco Embedded Wireless Controller on Catalyst Access Points in the network, they go through an internal protocol. The protocol selects one Cisco Embedded Wireless Controller on Catalyst Access Points, which is configured on the Cisco Wireless Controller as the primary AP to reach the PnP server.

Step 3 Find the unclaimed Cisco Embedded Wireless Controller on Catalyst Access Points in the **Provision > Network Devices > Plug and Play** tab.

The table lists all the unclaimed devices. The **State** column shows as **Unclaimed**. Use the **Filter** or **Find option** to find specific devices.

You must wait for the onboarding status to become **Initialized** under the **Onboarding State** column.

Step 4 To claim the Cisco Embedded Wireless Controller on Catalyst Access Points, check the check box next to the AP device name.

Step 5 Choose **Actions > Claim** in the menu bar above the device table.

The **Claim Devices** window is displayed.

Step 6 In the **Site Assignment** window, choose a site from the **Site** drop-down list.

Claiming the selected AP to this particular site also applies the associated configurations.

Step 7 Click **Next**.

Step 8 To configure a device, click the device name in the **Configuration** window.

Step 9 In the **Configuration for device name** window, assign the static IP details for the device.

Step 10 Click **Save**.

Step 11 Click **Next**.

The **Summary** window is displayed.

Step 12 Click **Claim** in the **Summary** window.

After the Cisco Embedded Wireless Controller on Catalyst Access Points is claimed, the IP address configured is assigned to the Cisco Embedded Wireless Controller.

The claimed device, which is a Cisco Embedded Wireless Controller with an internal AP, is now available under **Provision > Network Devices > Inventory**.

Step 13 To provision the additional controller, see [Provision a Cisco AireOS Controller, on page 391](#).

Step 14 To bulk import devices from a CSV file, see [Add Devices in Bulk, on page 375](#).

Step 15 To add devices manually, see [Add or Edit a Device](#).

Migrate Cisco AireOS Controller to Cisco Catalyst 9800 Series Wireless Controller Using Cisco DNA Center

Before you begin

- Design your network hierarchy by adding sites, buildings, and floors.
- Discover the Cisco Catalyst 9800 Series Wireless Controller by running the Discovery feature and add it to the Inventory. Make sure that the device status is reachable and in the Managed state.

You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete the configurations of network devices.
- Discover the Cisco AireOS Controllers and add it to the Inventory. Make sure that the device status is reachable and in the Managed state.

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window is displayed, which lists the discovered devices.

Step 2 Check the check box next to the Cisco AireOS Controller.

Step 3 From the **Actions** drop-down list, choose **Provision > Assign Device to Site**.

Step 4 In the **Assign Device to Site** window, click **Choose a Site**.

Step 5 In the **Add Sites** window, check the check box next to the site name to associate a Cisco AireOS Controller.

Step 6 Click **Save**.

Step 7 From the **Actions** drop-down list, choose **More > Learn Device Config**.

The **Site Assignment** window opens and the **Learn Device Configuration** workflow begins.

Note You can also start this workflow by doing the following:

- a. From the **Inventory** window, click the device's link to open a dialog box that provides high-level information for that device.
- b. Click **View Device Details** to open the device's details window.
- c. Click **Learn WLC Config**.

Step 8 In the **Assign Site** window, click **Next**.

Step 9 The **Resolve Conflict** window shows any conflicting configurations in Cisco DNA Center that you need to resolve. Click **Next**.

Step 10 In the **Design Object** window, click **Next**.

Step 11 In the left pane, click **Network**.

The right pane displays network configurations that were learned as part of the device configuration learning process, and shows the following information:

- AAA server details.
- Systems settings, with details about the IP address and protocol of the AAA server. Enter the shared secret for the AAA server because the passwords are encrypted and Cisco DNA Center cannot learn passwords.
- DHCP server, with details about all the DHCP servers available in the device.
- NTP server, with details about all the NTP servers available in the device.

Step 12 Click **Next**.

Step 13 In the left pane, click **Wireless**.

The **Wireless** window displays the enterprise SSIDs, guest SSIDs, wireless interfaces, and RF profiles that are present on the device.

Step 14 For an SSID with a preshared key (PSK), enter the passphrase key.

Step 15 In the left pane, click **Discarded Config**.

This displays the conflicting and the existing configurations on Cisco DNA Center. The discarded configuration entries are available under the following categories:

- Duplicate design entity
- Unknown device configuration for radio policy

Step 16 Click **Next**.

Step 17 The **Network Profile** window lists the network profile or site profile that is created based on the AP and WLAN combination.

Step 18 Click **Save**.

A success message is displayed.

- Step 19** Choose **Design > Network Settings > Wireless** to view the SSID and interface configurations that Cisco DNA Center has learned from the Cisco AireOS Controller.
- Step 20** Choose **Design > Network Profiles** to assign a site to the network profile.
- Step 21** In the **Network Profiles** window, click **Assign Site** to add sites to the selected profile.
- Step 22** In the **Add Sites to Profile** window, choose a site from the drop-down list, and click **Save**.
- Step 23** Click the **Provision** tab.
- Step 24** Check the check box next to the Cisco Catalyst 9800 Series Wireless Controller that you want to provision.
- Step 25** From the **Actions** drop-down list, choose **Provision**.
- Step 26** Click **Choose a site** to assign a site for the Cisco Catalyst 9800 Series Wireless Controller.
- Step 27** In the **Choose a site** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.
- Step 28** Click **Next**.
The **Configuration** window is displayed.
- Step 29** Select a role for the Cisco Catalyst 9800 Series Wireless Controller as **Active Main WLC**.
- Step 30** Click **Select Primary Managed AP Locations** to configure a managed AP location for the primary controller.
- Step 31** In the **Managed AP Location** window, check the check box next to the site name. You can either select a parent site or the individual sites. If you select a parent site, the children under that parent site are automatically selected.
- Step 32** Click **Save**.
- Step 33** Click **Next**.
- Step 34** The **Summary** window shows the configurations that will be pushed to the Cisco Catalyst 9800 Series Wireless Controller from the Cisco AireOS Controller.
- Step 35** Click **Deploy** to provision the Cisco Catalyst 9800 Series Wireless Controller.
- Step 36** Click **Now** to deploy the device immediately. Click **Later** to schedule deployment for a later time and click **Apply**.
- Step 37** After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.
- Step 38** In the **Device Inventory** window, click **See Details** in the **Provision Status** column to get more information about the network intent or to view a list of actions that you need to take.
- Step 39** To manually resynchronize the Cisco Catalyst 9800 Series Wireless Controller, on the **Provision > Inventory** window, select the controller that you want to manually synchronize.
- Step 40** From the **Actions** drop-down list, choose **Resync**.
- Step 41** Provision the AP.

Configure and Provision a Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches

Supported Hardware Platforms

Device Role	Platforms
Embedded Wireless Controller	Cisco Catalyst 9300 Series Switches

Device Role	Platforms
	Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches
Fabric Edge	Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500H Series Switches Cisco Catalyst 3600 Series Switches Cisco Catalyst 3850 Series Switches
APs	Cisco 802.11ac Wave 2 APs: <ul style="list-style-type: none"> • Cisco Aironet 1810 Series OfficeExtend Access Points • Cisco Aironet 1810W Series Access Points • Cisco Aironet 1815i Access Point • Cisco Aironet 1815w Access Point • Cisco Aironet 1815m Access Point • Cisco 1830 Aironet Series Access Points • Cisco Aironet 1850 Series Access Points • Cisco Aironet 2800 Series Access Points • Cisco Aironet 3800 Series Access Points • Cisco Aironet 4800 Series Access Points Cisco 802.11ac Wave 1 APs <ul style="list-style-type: none"> • Cisco Aironet 1700 Series Access Points • Cisco Aironet 2700 Series Access Points • Cisco Aironet 3700 Series Access Points Cisco Catalyst 9105 Series Wi-Fi 6 Access Points Cisco Catalyst 9115 Series Wi-Fi 6 Access Points Cisco Catalyst 9117 Series Wi-Fi 6 Access Points Cisco Catalyst 9120 Series Wi-Fi 6 Access Points Cisco Catalyst 9124 Series Wi-Fi 6 Access Points Cisco Catalyst 9130 Series Wi-Fi 6 Access Points Cisco Catalyst 9136 Series Wi-Fi 6 Access Points

Preconfiguration

On the Cisco Catalyst 9800 Series Wireless Controller, make sure that the following commands are present if the switch is already configured with **aaa new-model**:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

This is required for NETCONF configuration. These configurations are not required if you are using an automated underlay for provisioning.

Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches

1. Install Cisco DNA Center.
For more information, see the [Cisco DNA Center Installation Guide](#).
2. Log in to the Cisco DNA Center GUI and verify that the applications you need are in the **Running** state.
Click the menu icon (☰) and choose **System > Software Updates > Installed Apps**.
3. Integrate Cisco Identity Services Engine with Cisco DNA Center. After Cisco ISE is registered with Cisco DNA Center, any device that Cisco DNA Center discovers, along with relevant configurations and other data, is pushed to Cisco ISE.
4. Discover Cisco Catalyst 9000 Series Switches and the edge switches.
You must enable NETCONF and set the port to 830 to discover Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.
Do not enable NETCONF to discover the edge switches.
For more information, see [Discover Your Network Using CDP, on page 46](#) and [Discover Your Network Using an IP Address Range or CIDR, on page 48](#).
Change the **Preferred Management IP to Use Loopback**.
5. Make sure that the devices appear in the device inventory and are in **Managed** state.
For more information, see [About Inventory, on page 56](#) and [Display Information About Your Inventory, on page 57](#).
Ensure that the devices are in the **Managed** state.
6. Design your network hierarchy, which represents your network's geographical location. You can create sites, buildings, and floors so that later you can easily identify where to apply the design settings or configurations.
You can either create a new network hierarchy, or if you have an existing network hierarchy on Cisco Prime Infrastructure, you can import it into Cisco DNA Center.
To import and upload an existing network hierarchy, see the [Import Your Site Hierarchy to Cisco DNA Center, on page 128](#).

To create a new network hierarchy, see the [Create, Edit and Delete a Site, on page 134](#) and [Add, Edit, and Delete a Building, on page 135](#).

7. For a nonfabric network, add and position APs on a floor map to get heatmap visualization during the design phase.

For a fabric network, you cannot place APs on a floor map during the design time. The APs are onboarded after adding devices to a fabric network.

For more information, see [Work with APs on a Floor Map, on page 146](#).

8. Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network.

You can configure up to six AAA servers on the **Wireless** window during the SSID creation.

For more information, see [Network Settings Overview, on page 191](#), [Configure Global Network Servers, on page 193](#), and [Add Cisco ISE or Other AAA Servers](#).

9. Configure device credentials, such as CLI, SNMP, and HTTPS.

For more information, see [Global Device Credentials Overview, on page 194](#), [Configure Global CLI Credentials, on page 194](#), [Configure Global SNMPv2c Credentials, on page 195](#), [Configure Global SNMPv3 Credentials, on page 195](#), and [Configure Global HTTPS Credentials, on page 197](#).

10. Configure IP address pools at the global level.

To configure an IP address pool, see [Configure IP Address Pools, on page 202](#).

To reserve an IP address pool for the building that you are provisioning, see [Provision a Network Through LAN Automation](#).

11. Create enterprise and guest wireless networks. Define the global wireless settings once, and then Cisco DNA Center pushes the configurations to various devices across geographical locations.

Designing a wireless network is a two-step process. First, you must create SSIDs on the **Wireless** window. Then, associate the created SSID to a wireless network profile. This profile helps you to construct a topology, which is used to deploy devices on a site.

For more information, see [Create SSIDs for an Enterprise Wireless Network, on page 207](#) and [Create SSIDs for a Guest Wireless Network, on page 216](#).

12. Configure the backhaul settings.

13. Configure the following on the **Policy** window:

- Create a virtual network. The virtual network segments your physical network into multiple logical networks.
- Create a group-based access control policy, and add a contract. For more information, see [Create Group-Based Access Control Policy, on page 565](#).

14. Provision Cisco Catalyst 9000 Series Switches and the edge node switches with the configurations added during the design phase.

- Create a fabric site.
- Add devices to the fabric network by creating a CP+Border+Edge or CP+Border.

- Enable embedded wireless capabilities on the Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Series Switches.
- Onboard APs in the fabric site.

After the devices are deployed successfully, the deploy status changes from **Configuring** to **Success**.

Provision Embedded Wireless on Cisco Catalyst 9000 Series Switches

Before you begin

Before provisioning a Cisco Catalyst 9800 Embedded Wireless Controller on Catalyst 9000 Series Switches, ensure that you have completed the steps in [Configure Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9000 Switches, on page 433](#).

This procedure explains how to provision embedded wireless on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500H Series Switches.

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window is displayed with the discovered devices listed.

Step 2 Check the check box next to the Catalyst 9000 Series Switch device and an edge switch that you want to associate to a site.

Step 3 From the **Actions** drop-down list, choose **Provision > Assign Device to Site**.

Step 4 In the **Assign Device to Site** step, do the following:

- a) Click **Choose a site**.
- b) In the **Choose a site** slide-in pane, check the check box next to the site to associate the device.
- c) Click **Save**.
- d) Click **Apply**.

The next step is to provision the Catalyst 9000 Series Switch and the edge node with the configurations that were added during the design phase.

Step 5 In the **Devices > Inventory** window, check the check box next to the device name that you want to provision.

- a) From the **Actions** drop-down list, choose **Provision > Provision Device**.
- b) Click **Next**.
- c) In the **Summary** window, review the configuration, and click **Deploy**.
- d) In the **Provision Devices** window, do the following to preview the CLI configuration:

1. Click **Generate Configuration Preview** radio button.
2. In the **Task Name** field, enter a name for the CLI preview task, and click **Apply**.
3. In the **Task Submitted** dialog box, click the **Work Items** link.

Note This dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon (☰) and choose **Activities > Work Items**.

4. In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
5. View the CLI configuration details and click **Deploy**.

6. Click **Now** to deploy the device immediately or click **Later** to schedule the deployment for a later time and click **Apply**.

7. In the **Information** dialog box, do the following:

a. Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.

b. Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Step 6 To provision the edge switch, check the check box next to the edge switch that you want to provision.

a) From the **Actions** drop-down list, choose **Provision**.

b) Click **Next**.

c) In the **Summary** window, verify the configurations, and click **Deploy**.

After the devices are deployed successfully, the **Provision Status** changes from **Configuring** to **Success**.

Step 7 To add devices to a fabric site, click the menu icon (☰) and choose **Provision > Fabric Sites**.

Step 8 Create a fabric site. For more information, see [Add a Fabric Site, on page 473](#).

Step 9 Add an IP transit network.

Step 10 Add devices and associate virtual networks to a fabric site.

Step 11 Add the Cisco Catalyst 9000 Series Switch as a control plane, a border node, and an edge node or a control plane and a border node.

a) Click the device and choose **Add as CP+Border+Edge** or **Add as CP+Border**.

b) Click the edge node and choose **Add to Fabric**.

c) Click **Save**.

Step 12 To enable embedded wireless on the device, click the device that is added as a **Edge, CP+Border+Edge** or **CP+Border**, and click the **Embedded Wireless**.

a) If you have not installed the wireless package on Cisco Catalyst 9000 Series Switches before enabling the wireless functionality, a warning message is displayed by Cisco DNA Center: 9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually.

b) Click **OK** to install the image manually.

c) On the **Download Image** window, click **Choose File** to navigate to a software image stored locally, or **Enter image URL** to specify an HTTP or FTP source from which to import the software image.

d) Click **Import**.

The progress of the import is displayed.

e) Click **Activate image on device**.

A warning message is displayed: Activate image on device will reboot the device. Are you sure you want to reboot the device?

f) Click **Yes**.

The device reboots and comes online after the device package upgrade is complete.

g) In the dialog box, the AP locations that are managed by the controllers are displayed. You can change, remove, or reassign the site here.

h) Click **Next**.

- Step 13** In the **Summary** window, review the configuration settings, and click **Save**.
- Step 14** On the **Modify Fabric** step, click **Now** to commit the changes, and click **Apply** to apply the configurations. The next step is to onboard APs in a fabric site.
- Step 15** In the Cisco DNA Center GUI, click the **Provision** tab.
- Step 16** Click the **Fabric** tab.
A list of fabric sites is displayed.
- Step 17** Select the fabric site that was created, and click the **Host Onboarding** tab to enable IP pool for APs.
- Step 18** Select the authentication template that is applied for devices in the fabric site. These templates are predefined configurations that are retrieved from Cisco ISE. After selecting the authentication template, click **Save**.
- Step 19** Under **Virtual Networks**, click **INFRA_VN** to associate one or more IP pools with the selected virtual network.
- Step 20** Under **Virtual Network**, click the guest virtual networks to associate IP pools for the selected guest virtual network.
- Step 21** Check the **IP Pool Name** check box that was created for APs during the design phase.
- Step 22** Click **Update** to save the setting.
The AP gets the IP address from the specified pool, which is associated with the AP VLAN and registers with the Cisco wireless controller through one of the discovery methods.
- Step 23** Specify wireless SSIDs within the network that hosts can access. Under the **Wireless SSID** section, select the guest or enterprise SSIDs and assign address pools, and click **Save**.
- Step 24** Manually trigger resynchronization by performing an **Inventory > Resync** to see the APs on Cisco DNA Center for embedded wireless.
The discovered APs are now displayed under **Inventory** in the **Provision** window and the **Status** is displayed as **Not Provisioned**.
- Step 25** Provision the AP.
For more information, see [Provision a Cisco AP—Day 1 AP Provisioning, on page 397](#).
- Step 26** Configure and deploy application policies. For more information, see [Create an Application Policy, on page 602](#), [Deploy an Application Policy, on page 607](#), and [Edit an Application Policy, on page 606](#).
Provision the Catalyst 9300 Series Switches and Cisco Catalyst 9500H Series Switches before deploying an application policy.
Two different policies with different business relevance for two different SSIDs do not work. Always the last deployed policy takes precedence when you are setting up the relevance.
Changing the default business relevance for an application does not work in FlexConnect mode.
You can apply an application policy only on a nonfabric SSID.

Inter-Release Controller Mobility Introduction

Inter-Release Controller Mobility (IRCM) supports seamless mobility and wireless services across different Cisco Wireless Controllers with different software versions.

Cisco DNA Center supports the guest anchor feature for the following device combinations:

- Configuration of a Cisco AireOS controller as a foreign controller with a Cisco AireOS controller as an anchor controller.
- Configuration of a Cisco AireOS controller as a guest anchor controller with a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller.
- Configuration of a Cisco Catalyst 9800 Series Wireless Controller as a foreign controller with a Cisco Catalyst 9800 Series Wireless Controller as an anchor controller.

Configuring IRCM on controller devices has the following limitations:

- Configuration of a Cisco AireOS controller as a foreign controller and Cisco Catalyst 9800 Series Wireless Controller as an anchor controller is not supported.
- Configuration of a fabric guest anchor is not supported.
- Only guest SSID is supported.
- Broadcast of a nonguest anchor SSID in guest anchor mode is not supported.

Guest Anchor Configuration and Provisioning Process

Follow these steps to configure a guest anchor Cisco Wireless Controller.

-
- Step 1** Design a network hierarchy, with sites, buildings, floors, and so on. For more information, see [Create, Edit and Delete a Site, on page 134](#).
- Step 2** Configure network servers, such as AAA, DHCP, and DNS servers. For more information, see [Configure Global Network Servers, on page 193](#) and [Add Cisco ISE or Other AAA Servers, on page 192](#).
- Step 3** Create SSIDs for a guest wireless network with external web authentication and central web authentication along with configuring Cisco Identity Services Engine.
- Step 4** Discover the wireless controller using the Cisco Discovery Protocol (CDP) or an IP address range, and make sure that the devices are in the **Devices > Inventory** window and in the **Managed** state. For more information, see [Discovery Overview, on page 37](#).
- Step 5** Provision a foreign wireless controller as the active main wireless controller. See [Provision a Cisco AireOS Controller, on page 391](#).

Note If you choose a site with multiple network profiles while provisioning a foreign wireless controller, ensure that the total number of anchor groups for the network profiles is three or less.

- Step 6** Choose the role for the wireless controller as guest anchor and provision the guest anchor controllers. For more information, see [Provision a Cisco AireOS Controller, on page 391](#).

Note

- You must choose the same site as the managed AP location for the anchor wireless controller as specified for the SSID.
- If you modify the interface configuration for the anchor wireless controller, you must reprovise it.

- Step 7** Configure device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see [Configure Global CLI Credentials, on page 194](#), [Configure Global SNMPv2c Credentials, on page 195](#), [Configure Global SNMPv3 Credentials, on page 195](#), and [Configure Global HTTPS Credentials, on page 197](#).
-

Prerequisite for Configuring IRCM on Cisco Controller Device

- Discover the Cisco Catalyst 9800 Series Wireless Controller and Cisco AireOS Controllers.

You must enable NETCONF and set the port to 830 to discover the Catalyst 9800 Series Wireless Controller. NETCONF provides a mechanism to install, manipulate, and delete the configurations of network devices.

For more information, see [Discover Your Network Using CDP, on page 46](#) or [Discover Your Network Using an IP Address Range or CIDR, on page 48](#).

- Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations.

To create a new network hierarchy, see [Create, Edit and Delete a Site, on page 134](#) and [Add, Edit, and Delete a Building, on page 135](#).

- Add the location information of APs, and position them on the floor map to visualize the heatmap coverage.

For more information, see [Work with APs on a Floor Map, on page 146](#).

- Define network settings, such as AAA (Cisco ISE is configured for Network and Client Endpoint), NetFlow Collector, NTP, DHCP, DNS, syslog, and SNMP traps. These network servers become the default for your entire network. You can add a TACACS server while adding a AAA server.

For more information, see [Network Settings Overview, on page 191](#), [Configure Global Network Servers, on page 193](#), and [Add Cisco ISE or Other AAA Servers](#).

- Create SSIDs for a guest wireless network.


For more information, see [Create SSIDs for a Guest Wireless Network, on page 216](#).

- The WLAN profile name of the foreign controller and anchor controller should be the same for mobility.

IRCM: Cisco AireOS Controller and Cisco Catalyst 9800 Series Wireless Controller

Before you begin

Ensure the prerequisite for configuring IRCM is met. For more information, see [Prerequisite for Configuring IRCM on Cisco Controller Device, on page 439](#).

- Step 1** Click the menu icon () and choose **Provision > Network Devices > Inventory**.
The **Inventory** window is displayed with the discovered devices listed.

- Step 2** Check the check box next to the Catalyst 9800 Series Wireless Controller that you want to provision as a foreign controller.
- Step 3** From the **Actions** drop-down list, choose **Provision > Provision**.
- Step 4** In the **Assign Site** window, click **Choose a Site** to assign a site for the Catalyst 9800 Series Wireless Controller device.
- Step 5** In the **Add Sites** window, check the check box next to the site name to associate a Catalyst 9800 Series Wireless Controller.
- Step 6** Click **Save**.
- Step 7** Click **Apply**.
- Step 8** Click **Next**.
- Step 9** Select a role for the Catalyst 9800 Series Wireless Controller as **Active Main WLC**.
- Step 10** For an active main wireless controller, you need to configure interface and VLAN details.
- Step 11** Under the **Assign Interface** area, do the following:
- VLAN ID**: Enter a value for the VLAN ID.
 - IP Address**: Enter the interface IP address.
 - Gateway IP Address**: Enter the gateway IP address.
 - Subnet Mask (in bits)**: Enter the interface net mask details.
- Note** Assigning an IP address, gateway IP address, and subnet mask is not required for the Catalyst 9800 Series Wireless Controller.
- Step 12** Click **Next**.
- Step 13** In the **Summary** window, review the configuration settings.
- Step 14** Click **Deploy** to provision the Catalyst 9800 Series Wireless Controller as a foreign controller.
- Step 15** On the **Devices > Inventory** window, check the check box next to the Cisco AireOS Controller that you want to provision as a guest anchor controller.
- Step 16** Repeat Step 3 through Step 8.
- Step 17** Select a role for the Cisco AireOS Controller as **Guest Anchor**.
- Step 18** For a guest anchor wireless controller, you need to configure the interface and VLAN details.
- Step 19** Repeat Step 11 through Step 14.
-

Prerequisites for Provisioning a Meraki Device

- Integrate the Meraki dashboard with Cisco DNA Center. See [Integrate the Meraki Dashboard, on page 87](#).
- Create the SSID. See [Create SSIDs for an Enterprise Wireless Network, on page 207](#).



-
- Note** The Meraki dashboard supports the following types of SSIDs:
- Open: This SSID corresponds to Open in the Meraki dashboard.
 - WPA2 Personal: This SSID corresponds to the preshared key with WAP2 in the Meraki dashboard.
 - WPA2 Enterprise: This SSID corresponds to WAP-2 Encryption with Meraki authentication or My Radius server in the Meraki dashboard. If you have defined AAA or Cisco ISE servers for client and endpoint authentication at the building level in Cisco DNA Center, the configuration is provisioned to **my Radius server** in the Meraki dashboard. Otherwise, **Meraki Radius** is used for authentication by the Meraki devices.

For every SSID, you can choose an interface name. If you choose the **Management** interface in Cisco DNA Center and the VLAN ID is 0, the configuration is not supported in the Meraki dashboard and VLAN tagging is disabled in the Meraki dashboard. If you create a custom interface for the SSID in Cisco DNA Center, an AP tag is created with the custom interface name and VLAN ID in the Meraki dashboard.

-
- Create the network profile and assign it to the sites for which the SSID is provisioned.



-
- Note** The Network Hierarchy **Sites > Buildings** in Cisco DNA Center corresponds to **Organization > Network** in the Meraki dashboard. We recommend that you choose **Buildings** in the **Add Sites to Profile** window in the workflow.
-



-
- Note** Cisco DNA Center creates the Meraki network and provisions the SSIDs to the network. The Meraki dashboard provisions the Meraki network configuration to the Meraki devices.
-

Provision a Meraki Device

This procedure explains how to provision SSIDs to Cisco Meraki devices managed by a Meraki dashboard.

Before you begin

Ensure the prerequisite is met. For more information, see [Prerequisites for Provisioning a Meraki Device, on page 440](#).

Step 1 Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.

The **Inventory** window is displayed with the discovered devices listed.

Step 2 To view the Meraki dashboard, expand the **Global** site in the left pane, and select a building.

All Meraki dashboards available in the selected building are displayed.

Step 3 Check the check box next to the Meraki dashboard name that you want to provision.

Step 4 From the **Actions** drop-down list, choose **Provision > Provision Device**.

The **Assign Site** window is displayed, which is where you can view the Meraki dashboard and the associated building.

Step 5 To change the associated building, click **Choose a site**.

Step 6 In the **Choose a site** window, select a building and click **Save**.

Step 7 Click **Next**.

The **Configuration** window is displayed. You can view the managed building in the primary location.

Step 8 Click **Select Secondary Managed AP Locations** to select the secondary managed location for the Meraki dashboard.

Step 9 In the **Managed AP Location** window, check the check box next to the building name.

Step 10 Click **Save**.

Step 11 Click **Next**.

In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Note Meraki deployment supports a maximum of 15 SSIDs in each network.

Step 12 Click **Deploy**.

Step 13 In the **Provision Devices** window, do the following to preview the CLI configuration:

- Click the **Generate Configuration Preview** radio button.
- In the **Task Name** field, enter a name for the CLI preview task, and click **Apply**.
- In the **Task Submitted** dialog box, click the **Work Items** link.

Note This dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon (☰) and choose **Activities > Work Items**.

- In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- View the CLI configuration details, and click **Deploy**.
- To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- In the **Information** dialog box, do the following:
 - Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
 - Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

The **Provision Status** column in the **Device Inventory** window shows `SUCCESS` after a successful deployment.

Provision Remote Teleworker Devices

The following topics explain the components of remote teleworker sites and the procedure for provisioning remote teleworker devices.

Remote Teleworker Deployment Overview

Deployment Components

The Cisco remote teleworker deployment is built around three main components: Cisco wireless controllers, Cisco OfficeExtend access points (APs) and a Corporate firewall. The following models are supported in this deployment:

- **Wireless Controllers:** Cisco 5520 Wireless Controller, Cisco 8540 Wireless Controller, Cisco 3504 Wireless Controller⁴, Cisco Catalyst 9800-40 Wireless Controller, Cisco Catalyst 9800-80 Wireless Controller, and Cisco Catalyst 9800-L Wireless Controller.
- **Access Points:** Cisco Aironet 1815T (Teleworker) Access Point, Cisco Aironet 1815I Access Point, Cisco Aironet 1815W Access Point, Cisco Aironet 1840I Access Point, Cisco Aironet 2800 Series Access Points, Cisco Aironet 3800 Series Access Points, Cisco Aironet 4800 Series Access Points, Cisco Catalyst 9115 Access Point, Cisco Catalyst 9120 Access Point, and Cisco Catalyst 9130 Access Point.

Cisco Wireless Controllers

Cisco controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco APs to support business-critical wireless applications for teleworkers. Controllers provide the control, scalability, security, and reliability that network managers need to build a secure, scalable teleworker environment.

To allow users to connect their corporate devices to the organization's on-site wireless network, the remote teleworking solution offers the same wireless Secure Set Identifiers (SSIDs) at a teleworker's home as those that support data and voice inside the organization.

Cisco OfficeExtend Access Points

APs cannot act independently of controllers. As an AP communicates with the controller resources, it downloads its configuration and synchronizes its software or firmware image, if required. The AP establishes a secure Datagram Transport Layer Security (DTLS) connection to the controller, which offers remote WLAN connectivity using the same profile as at the corporate office. Secure tunneling allows all traffic to be validated against centralized security policies and minimizes the management overhead associated with home-based firewalls.

Corporate Firewall

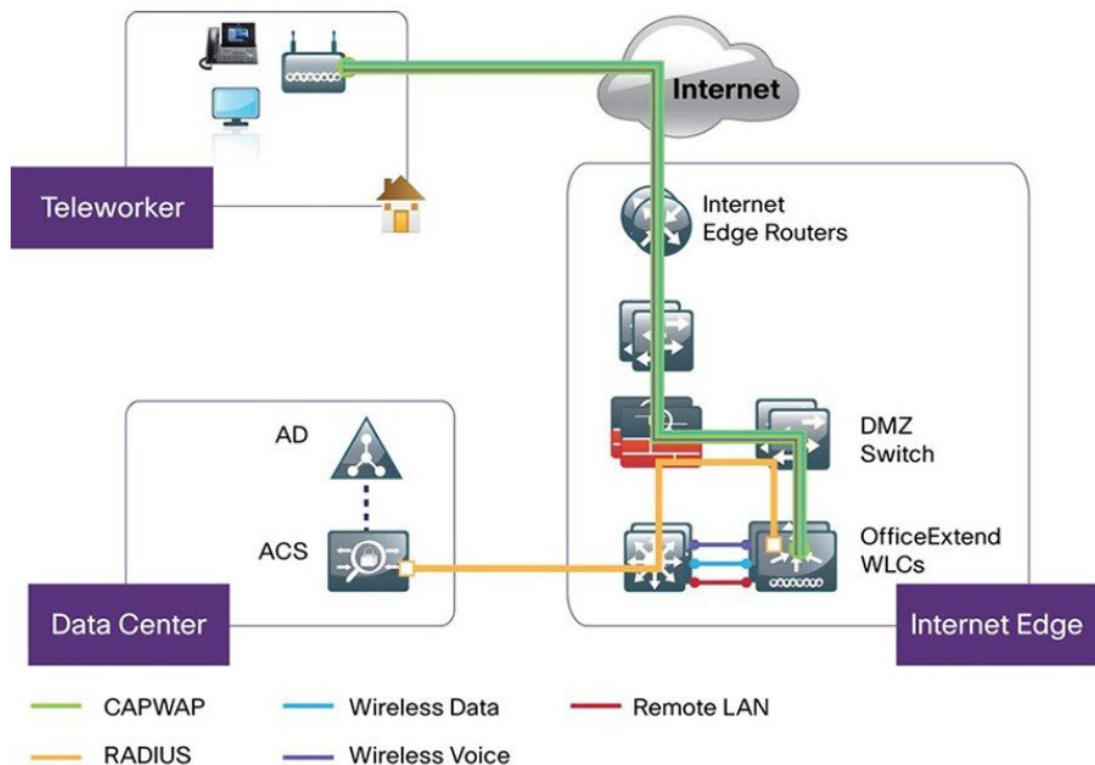
The controller should be placed in a demilitarized zone (DMZ) and the corporate firewall must allow CAPWAP control and data traffic through the firewall to the controller. The general configuration on the firewall is to allow CAPWAP control and CAPWAP management port numbers through the firewall. The UDP 5246 and 5247 ports need to be opened on the firewall for communication between the controller and the AP.

⁴ Supported with Cisco Aironet 1815 Teleworker Access Point only.

Deployment Configuration

For the most flexible and secure remote teleworker configuration, deploy a dedicated controller pair in a dedicated to the Internet edge DMZ. Traffic from the Internet terminates in the DMZ versus in the internal network, while the remote AP is still directly connected to the internal network.

Figure 21: Sample Remote Teleworker Deployment Scenario



Create a Remote Teleworker Site

A remote teleworker site is a dedicated site that is used only to manage wireless controllers and remote teleworker access points (APs). To create a remote teleworker site, you need to enable the remote teleworker function on the site. Once enabled, the remote teleworker function cannot be independently disabled for a site, building, or floor within the site's hierarchy. The site can only manage remote teleworker functions.

In a teleworker site, switching is performed centrally from the controller. You cannot configure the network profile for Flex Connect with local switching.

Before you begin

- Understand the supported devices that are used in a teleworker deployment.
- Make sure that you have a Cisco wireless controller and Cisco APs in your inventory. If not, discover the devices or add them manually. For information, see [Discover Your Network, on page 37](#) or [Add a Network Device, on page 73](#).
- Configure global wireless network settings appropriate for your network. For information, see [Configure Global Wireless Settings, on page 207](#).

- We recommend that you create an AP profile with remote teleworker enabled and configure custom site tags. For more information, see [Configure Additional Settings for an AP Profile for Cisco IOS XE Devices, on page 259](#) and [Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 285](#).
- For Cisco AireOS devices, you must map the AP profile to the custom AP group of the site that will be used for the remote teleworker AP. For more information, see [Create Network Profiles for Wireless, on page 281](#) and [Add AP Groups, Flex Groups, Site Tags, and Policy Tags to a Network Profile, on page 285](#).

Step 1 Create a site to manage remote teleworker APs. See [Create, Edit and Delete a Site, on page 134](#).

Step 2 Add buildings and floors. See [Add, Edit, and Delete a Building, on page 135](#).

Step 3 Configure the wireless network settings for the remote teleworker site.

- a) Click the menu icon (☰) and choose **Design > Network Settings > Wireless**.
- b) From the left hierarchy tree, choose the remote teleworker site.
- c) Scroll down and check the **Enable Remote Teleworker** check box.
- d) Click **Save**.

Step 4 Assign the controller to the site. See [Add a Device to a Site, on page 90](#).

Step 5 Assign the APs to the site. See [Add a Device to a Site, on page 90](#).

You can use serial numbers or MAC addresses but not a mixture of both, or you can upload a CSV file.

Step 6 In the wireless network settings, add the APs to the authorized APs list.

- a) From the left hierarchy tree, choose Global.
- b) Click the menu icon (☰) and choose **Design > Network Settings > Wireless**.
- c) Under **Authorized Access Points**, click **Manage Authorized Access Points**.
- d) In the **Manage Authorized Access Points** pane, identify the APs that are allowed to join the controller by entering the AP's MAC address, serial number, or both.

The controller responds only to CAPWAP requests from APs that are in its authorization list.

Step 7 Provision the controller.

- a) Click the menu icon (☰) and choose **Provision > Inventory**.
The Inventory window is displayed with the discovered devices listed.
- b) Locate the controller that you want to provision.
- c) Check the check box next to the device name.
- d) From the **Actions** drop-down list, choose **Provision > Provision Device**.
- e) In the **Assign Site** window, verify the assigned site, and click **Save**.
- f) Click **Next**.
- g) (Optional) On the **Configuration** window, under **NAT Address for Remote Teleworker**, click the **Enable NAT Address** check box and enter the NAT IP address.
- h) Click **Next**.
- i) In the **Model Configuration** window, click **Next**.
- j) In the **Advanced Configuration** window, click **Next**.
- k) In the **Summary** window, review the configuration settings, and click **Deploy**.
- l) In the **Provision Device** slide-in pane, choose **Now**, and click **Apply**.

Step 8 After the Cisco Wireless Controller is provisioned, you can provision the APs.

- a) Click the menu icon (☰) and choose **Provision > Inventory**.

The **Inventory** window is displayed with the discovered devices listed.

- b) Locate the APs that you want to provision.
 - c) Check the check box next to the device names.
 - d) From the **Actions** drop-down list, choose **Provision > Provision Device**.
 - e) In the **Assign Site** window, click **Choose a floor**, and assign the APs to a floor.
 - f) Click **Save**.
 - g) Click **Next**.
 - h) In the **Configuration** window, click **Next**.
 - i) In the **Summary** window, review the configuration settings, and click **Deploy**.
 - j) In the **Provision Device** slide-in pane, choose **Now**, and click **Apply**.
-



CHAPTER 18

Provision a Routing Profile

- [Provision a Router, on page 447](#)
- [VPC Inventory Collection, on page 449](#)

Provision a Router

Before you begin

Make sure that you have defined the following global network settings before provisioning a routing profile:

- Network servers, such as AAA, DHCP, and DNS. For more information, see [Configure Global Network Servers, on page 193](#).
- Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see [Configure Global CLI Credentials, on page 194](#), [Configure Global SNMPv2c Credentials, on page 195](#), [Configure Global SNMPv3 Credentials, on page 195](#), and [Configure Global HTTPS Credentials, on page 197](#).
- IP address pools. For more information, see [Configure IP Address Pools, on page 202](#).
- SP profiles. For more information, see [Configure Service Provider Profiles, on page 207](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The **Inventory** window is displayed with the discovered devices listed.
- Step 2** To view devices available in a particular site, expand the Global site in the left pane, and select the site, building, or floor that you are interested in.
All the devices available in that selected site are displayed in the **Inventory** window.
- Step 3** From the **Device Type** list, click the **Routers** tab, and from the **Reachability** list, click the **Reachable** tab to get a list of devices that are discovered and reachable.
- Step 4** Check the check box next to the device name that you want to provision.
- Step 5** Click **Assign** under the site; the **Assign Device to Site** window is displayed. Click **Choose a Site**.
- Step 6** From the **Actions** drop-down list, choose **Provision > Provision Device**.
To provision a router, do the following:

- a. Review the details in the **Confirm Profile** window, and click **Next**.
- b. Review the details in the **Router WAN Configuration** window.
 1. If you selected Gigabit Ethernet as the line interface, click **O** and enter the WAN IP address if you select a static IP address. If you select DHCP, enter the IP address from the DHCP server. If the primary WAN is already configured using PnP, you can select **Do not Change** and select the interface that is configured as the primary WAN from the drop-down list.
 2. If you selected cellular as the line interface, click **O**, choose **IP Negotiated**, select the **Interface Name** from the drop-down list, and enter the **Access Point Name (APN)**. Depending on your service provider, check the **PAP** or **CHAP** check box.
 3. Enter the **IP SLA Address** for the backup WAN interface when you have multiple service providers.


This window does not appear if you are provisioning a virtual router.

- c. Review the details in the **Router LAN Configuration** window, and click **Next**.
You can now select one L3 interface or one or multiple L2 interfaces from the **Interface(s)** drop-down list.
- d. Review the details in the **Integrated Switch Configuration** window, and click **Next**.
- e. Review the details in the **Summary** window.

Step 7 Click **Deploy**.

Step 8 In the **Provision Devices** window, do the following to preview the CLI configuration:

- a. Click the **Generate Configuration Preview** radio button.
- b. In the **Task Name** field, enter a name for the CLI preview task and click **Apply**.
- c. In the **Task Submitted** dialog box, click the **Work Items** link.

Note This dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon () and choose **Activities > Work Items**.
- d. In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.
- e. View the CLI configuration details and click **Deploy**.
- f. To immediately deploy the device, click the **Now** radio button, and click **Apply**.
- g. To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.
- h. In the **Information** dialog box, do the following:
 1. Click **Yes** if you want to delete the CLI preview task from the **Work Items** window.
 2. Click **No** if you want to retain the task in the **Work Items** window.

Note The CLI task will be marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

The **Provision Status** column in the **Device Inventory** window shows **SUCCESS** after a successful deployment. Click **SUCCESS** to see a detailed provisional log status.

VPC Inventory Collection

After successful cloud inventory collection, the **Cloud** tab in the **Provision** section provides a view of the collected AWS VPC Inventory. The navigation on the left can be expanded to show the cloud regions for a cloud profile or access key. You can filter the left navigation items by keyword and click to see the VPCs just for the selected region or access key.

In the VPC Inventory view you can also click on a VPC to see more details about it, like the subnets and virtual instances in that VPC and some more details about them. AWS VPC inventory collection is scheduled to occur at the default interval for all inventory collection and can also be triggered on demand by using the **Sync** action from the gear menu for a cloud access key. The status of the inventory collection can be viewed by clicking on **Show Sync Status** in the **VPC Inventory** view.



CHAPTER 19

Provision Firewall Profiles

- [Provision a Firewall Threat Defense Device, on page 451](#)

Provision a Firewall Threat Defense Device

This procedure explains how to provision a Firepower Threat Defense (FTD) device managed by Firepower Management Center (FMC).

Before you begin

- Integrate FMC with Cisco DNA Center. See [Integrate Firepower Management Center, on page 88](#).
- Create a site in a network hierarchy. See [Create, Edit and Delete a Site, on page 134](#).
- Create a network profile for firewall and assign it to a site for which the FTD device is provisioned. See [Create Network Profiles for Firewall, on page 277](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Network Devices > Inventory**.
The Inventory page displays the device information that is gathered during the discovery process.
- Step 2** Check the check box next to the FTD device that you want to provision and click **Assign** under the **Site** column.
- Step 3** In the **Assign Device to Site** window, click **Choose a Site**.
- Step 4** In the **Choose a Site** window, select a site from the hierarchy and click **Save**.
- Step 5** Click **Next**.
- Step 6** Click **Now** to assign the device to site immediately or click **Later** to schedule at a specific time.
- Step 7** Click **Assign**.
- Note** You can view the status of assigning device to site in **Activities > Tasks**.
- Step 8** From the **Actions** drop-down list, choose **Provision > Provision Device**.
The **Provision Firewall Profile** window appears.
- Step 9** Review the details in the **Confirm Profile** page and click **Next**.
- Step 10** Review the details in the **Firewall Type** page and click **Next**.

The **FTD Configuration** page appears.

Step 11

If you have associated a routed mode firewall with the site, do the following:

- a) Expand the **Outside Interface** area, choose an outside interface from the **Select Physical Interface** drop-down list, and choose **Static IP** or **DHCP** radio button.
 - **Static IP:** Enter the IP address and a subnet mask.
 - **DHCP:** The IP address is obtained from DHCP.
- b) Expand the **Inside Interface** area, choose an inside interface from the **Select Physical Interface** drop-down list, and choose **Static IP** or **DHCP** radio button.
 - **Static IP:** Enter the IP address and a subnet mask.
 - **DHCP:** The IP address is obtained from DHCP.

Step 12

If you have associated a transparent mode firewall with the site, do the following:

- a) Expand the **Outside Interface** area and choose an outside interface from the **Select Physical Interface** drop-down list.
- b) Expand the **Inside Interface** area and choose an inside interface from the **Select Physical Interface** drop-down list.
- c) Expand the **Bridge Virtual Interface** area, and do the following:
 - **Bridge Group Number:** Enter a bridge group number. The valid number is from 1 to 250.
 - **IP:** Enter the IP address of the FTD device.
 - **Subnet Mask:** Enter a subnet mask.

Step 13

Click **Next**.

Step 14

In the **Summary** window, review the device specifications.

Step 15

To proceed, click **Deploy**.

The **Provision Firewall device(s)** dialog box appears.

Step 16

Click **Now**, **Later**, or **Generate configuration preview** radio button.

- **Now:** Starts the provision immediately.
- **Later:** Schedules the provisioning at a specific time.
- **Generate configuration preview:** Generates preview which can be later used to deploy on selected devices.

Step 17

Click **Apply**.

Note You can view the status of provisioning firewall device in **Activities > Tasks**. If you have chosen **Generate configuration preview** in the **Provision Firewall device(s)** dialog box, you can view the status in **Activities > Work Items**.



CHAPTER 20

Provision a LAN Underlay

- [LAN Automation, on page 453](#)
- [Prerequisites for Provisioning a Network Through LAN Automation, on page 454](#)
- [Provision a Network Through LAN Automation, on page 455](#)
- [Peer Device in LAN Automation Use Case, on page 458](#)
- [Check the LAN Automation Status, on page 460](#)
- [Create a Link Between Interfaces, on page 460](#)
- [Delete a Link Between Interfaces, on page 461](#)

LAN Automation

Cisco DNA Center provides LAN automation as an alternative for manual deployment of new networks. It allows you to simplify network operations and create a standard error-free network. LAN automation uses the IS-IS routing protocol to deploy a Layer 3 routed access design.

The **LAN Automation** window provides the capabilities to do the following:

- Provision your network through LAN automation.
- View the history of LAN automation sessions.
- View the summary for LAN automated devices.

Click the menu icon (☰) and choose **Provision > LAN Automation** to view this window.

- **Start LAN Automation:** Use this option to initiate LAN automation sessions on your network.
- **Overview:** Expand this section to view the prerequisites and more information about provisioning your network through LAN automation.
- **Sessions:** This section consists of the **History** and **LAN Automated Devices** tabs.

Day 0 Operation

On day 0, click **Start LAN Automation** to start provisioning your network through LAN automation. For more information, see [Provision a Network Through LAN Automation, on page 455](#).

For day 0, Cisco DNA Center doesn't display any data in the **Sessions** section.

Day *n* Operation

On day *n*, you can click **Start LAN Automation** to initiate more LAN automation sessions. You can run up to five LAN automation sessions simultaneously across sites. For more information, see [Provision a Network Through LAN Automation, on page 455](#).

When a LAN automation session is in progress, Cisco DNA Center displays a tile for the session in the **LAN Automation** window. To view the details of the session, click **See Session Details** in the tile. To stop LAN automation for the session, click **Stop LAN Automation** in the tile.

The **History** tab displays the history of LAN automation sessions in your network. You can use the search field to search for specific text in history. Click the hyperlinked date to view the session details. To view the logs for a session, in the session details window, click **View Session Logs**.

The **LAN Automated Devices** tab displays the details of the LAN automated devices. You can use the search field to filter the data based on specific text. Click one of the following toggle buttons to filter the data:

- **Seed Devices:** Displays the data for seed devices
- **Discovered:** Displays the data for discovered devices
- **Provisioned:** Displays the data for provisioned devices
- **Error:** Displays the data for devices with errors

In the **LAN Automated Devices** tab, you can also do the following:

- Click the device name hyperlink to view the device details.
- Provision interfaces between two devices using the **Add Link** option. For more information, see [Create a Link Between Interfaces, on page 460](#).
- Delete the interface between two devices using the **Delete Link** option. For more information, see [Delete a Link Between Interfaces, on page 461](#).

Prerequisites for Provisioning a Network Through LAN Automation

Before provisioning a network through LAN automation, ensure the following:

- Configure your network hierarchy. (See [Add a Device to a Site, on page 90](#).)
- Make sure you have defined the following global network settings:
 - Network servers, such as AAA, DHCP, and DNS servers. (See [Configure Global Network Servers, on page 193](#).)
 - Device credentials, such as CLI, SNMP, HTTP, and HTTPS credentials. (See [Configure Global CLI Credentials, on page 194](#), [Configure Global SNMPv2c Credentials, on page 195](#), [Configure Global SNMPv3 Credentials, on page 195](#), and [Configure Global HTTPS Credentials, on page 197](#).)



Note SNMPv2 write credentials are not required and if configured, it won't be pushed to the device during LAN automation.

- IP address pools. (See [Configure IP Address Pools](#), on page 202.)
- Make sure that you have at least one device in your inventory. If not, discover devices using the Discovery feature.



Note LAN automation is blocked if the discovered site is configured with CLI credentials that has a username "cisco".

- If you have a Cisco Catalyst 9400 Switch configured in the network, ensure that the following operations are done on the switch for LAN automation to automatically enable the 40G port:
 - [Day-0 Configuration](#) is performed on the switch.
 - A 40G Quad Small Form-Factor Pluggable (QSFP) transceiver is inserted in either port 9 or port 10 of the Supervisor, and the ports numbered 1 to 8 on the Supervisor do not have a 10G or 1G Small Form-Factor Pluggable (SFP) transceiver inserted in them. If there are dual supervisor engines, ensure that the 40G QSFP is inserted in port 9.

For more information on the Catalyst 9400 Series Supervisor, see [Cisco Catalyst 9400 Series Supervisor Installation Note](#).


Provision a Network Through LAN Automation

Before you begin

Make sure that the prerequisites have been met. For more information, see [Prerequisites for Provisioning a Network Through LAN Automation](#), on page 454.

Step 1 Reserve an IP address pool for the site that you are provisioning.

Note The size of the LAN automation IP address pool must be at least 25 bits of netmask or larger.

- Click the menu icon () and choose **Design > Network Settings > IP Address Pools**.
- In the **Network Hierarchy** pane, choose a site.
- Click **Reserve** and provide information in the following fields in the **Reserve IP Pool** window to reserve all or part of an available global IP address pool, for the specific site:
 - **IP Address Pool Name:** Unique name for the reserved IP address pool.
 - **Type:** Type of IP address pool. For LAN automation, choose **LAN**.
 - **IP Address Space:** Check either the **IPv4** or the **IPv6** check box to create an address pool. To create a dual-stack pool, check both the **IPv4** and **IPv6** check boxes.
 - **Global IP Pool:** IPv4 address pool from which you want to reserve all or some of the IP addresses.

Note LAN automation uses only the IPv4 subnet.

- **Prefix length / Number of IP Addresses:** IP subnet and mask address that is used to reserve all or part of the global IP address pool or the number of IP addresses that you want to reserve.
- **Gateway:** Gateway IP address.
- **DHCP Server(s):** DHCP server IP address.
- **DNS Server(s):** DNS Server IP address.

d) Click **Reserve**.

Step 2 Initiate the discovery and provisioning of the devices:

- a) Click the menu icon (☰) and choose **Provision > LAN Automation**.
- b) In the **LAN Automation** window, click **Start LAN Automation**.

The LAN Automation workflow guides you through the configuration process.

Step 3 In the **Seed Devices** window, do the following:

- Select the Primary Seed Device and its interface.
- (Optional) Select the Secondary Seed Device and its interface.

Step 4 In the **Sessions Attributes** window, do the following:

- Select the site to which all the newly discovered devices are assigned. This site can be different from the primary and peer sites.
- Select the IP Address Pool from the **Principal IP Address Pool** drop-down.
- (Optional) Click the **Advance Attributes** toggle button to set the IS-IS Password and also to enable multicast.
- In the HOSTNAME MAPPING section, define a prefix name for the devices in the **Discovered Devices Hostname Prefix** field.

You can either select a hostname map file from the **Choose a File** drop-down, or upload the .csv file from storage.

- Click **Review**.

Step 5 In the **Review** window, look through all the LAN Automation session settings. To make any changes, click **Edit**.

Click **Start**.

The following table describes each field that you see in the LAN Automation workflow window:

Primary Seed Device	Select the primary device that Cisco DNA Center uses as the starting point to discover and provision new devices.
Secondary Seed Device	Select the secondary seed device.
Discovered Device Site	All the newly discovered devices are assigned to this site. This site can be different from the primary and peer sites.
Principal IP Pool	IP address pool that was reserved for LAN automation.

Link Overlapping IP Pool	<p>IP address pool that is shared with other sites and is used to configure the /31 IP addresses on point-to-point links in the underlay.</p> <ul style="list-style-type: none"> • A link that overlaps IP pool can be a subpool that is inherited from a parent site or a subpool that is defined in any other site. • A link that overlaps IP pool allows you to overlap /31 IP addresses in a multisite deployment. Hosts in different sites will be able to reuse the IP addresses on the /31 links. • If you choose to define a link that overlaps IP pool, the addresses that are defined in the Principal IP Pool field are used for management IPs such as loopback address, VLAN address, and so on.
IS-IS Domain Password	<p>A user-provided IS-IS password when LAN automation starts. If the password exists on the seed device, it is reused and is not overwritten. If no user-provided password is entered and there is no existing IS-IS password on the device, the default domain password is used. If both the primary and the secondary seeds have domain passwords, ensure that they match.</p>
Advertise LAN Automation summary route into BGP	<p>Check this check box if you want LAN automation to advertise the Principal IP pool into BGP on the primary and peer seed device. LAN automation advertises the summary route on the seed devices only if BGP is configured on them.</p> <p>This check box is disabled by default. It is enabled only if the primary or the peer seed device has an autonomous system (AS) number configured.</p>
Enable Multicast	<p>Check this check box to enable underlay native multicast. LAN automation creates a multicast tree with seed devices as RPs and discovered devices as subscribers.</p>
Choose a File	<p>Click Browse to choose a hostname map file. User-provided names are configured for discovered devices using the chosen CSV file that contains a mapping between serial numbers and hostnames. If the discovered device is a stack, all the serial numbers of the stack are provided in the CSV file.</p> <p>A sample CSV file is as follows:</p> <pre>standalone-switch,FCW2212L0NF stack-switch,"FCW2212E00Y,FCW2212L0GV"</pre>

Device Name Prefix	Name prefix for the devices being provisioned. When Cisco DNA Center provisions each device, it prefixes the device with the text that you provide and adds a unique number at the end. For example, if you input "Access" as the name prefix, each consecutive device that is provisioned is named Access-1, Access-2, Access-3, and so on.
--------------------	--

Cisco DNA Center begins to discover and provision the new devices.

LAN automation configures an IP address on the seed device of VLAN 1. If this VLAN 1 IP address of the seed device is not reachable from Cisco DNA Center, an error message is displayed on the **LAN Automation Status** window. Hover your cursor over the **See Details** link on this window to see the error details and possible remedial actions.

Step 6 Monitor and review the progress of the devices being provisioned.

a) In the **LAN Automation** window, click **See Session Details** on the status pane.

You can filter the status display and see the details of the discovered devices, or the provisioned devices, or error messages.

Note The provisioning of new devices may take several minutes.

b) After all the devices have been discovered and added to the inventory, click **Stop LAN Automation** in the **LAN Automation Status** window.

The LAN automation process is complete, and the new devices are added to the inventory.

Step 7 (Optional) You can have multiple LAN Automation sessions (up to five sessions) running in parallel. The details of each session are displayed on the respective tiles in the LAN Automation window.

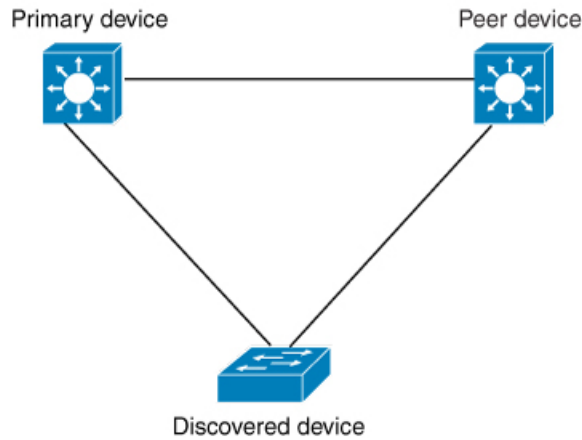
Consider the following aspects before you start simultaneous LAN Automation sessions:

- You can't use the same seed device for more than one session.
- You can't use the same site for parallel sessions.
- You can't use the same IP Pool for parallel sessions.

Peer Device in LAN Automation Use Case

Provision a Dual-Homed Switch

You must always select a peer device to provision the dual-homed switch.



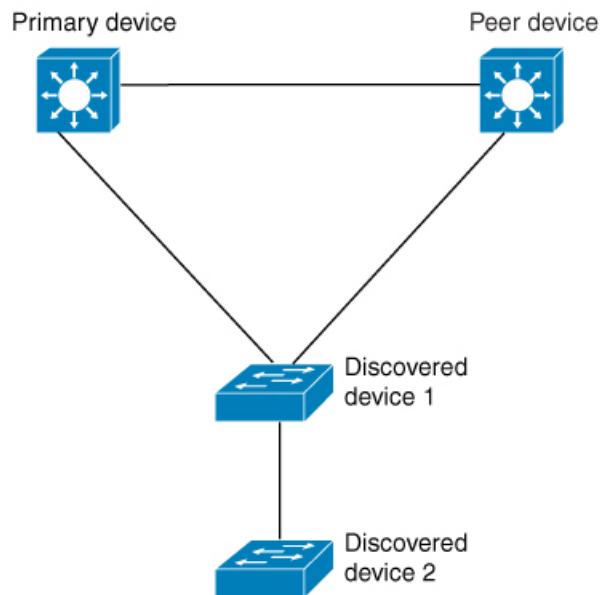
355771

Cisco DNA Center configures the DHCP server on the primary device. Because Cisco DNA Center understands that the discovered device is connected to both the primary and peer devices, it configures two Layer 3 point-to-point connections when the LAN automation task is stopped. One connection is established between the discovered device and the primary device; the other connection is established between the discovered device and the peer device.



Note If the link between the primary and the peer device is not configured before the LAN automation job is executed, you must select the interface of the primary device that connects to the peer device as part of the LAN automation configuration in Cisco DNA Center.

LAN Automation's Two-Hop Limitation



355772

For the preceding topology, Cisco DNA Center configures the following links:

- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Primary device*
- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Peer device*
- A point-to-point Layer 3 routed connection from *Discovered device 1* to *Discovered device 2*

Consider the scenario where a device—named *Discovered device 3*—is directly connected below *Discovered device 2*. The connection between *Discovered device 2* and *Discovered device 3* is not configured as part of the LAN automation job, because it is more than two hops away from *Primary device*.

Check the LAN Automation Status

You can view the status of in-progress LAN automation jobs.

Before you begin

You must have created and started a LAN automation job.

-
- Step 1** Click the menu icon (☰) and choose **Provision > LAN Automation**.
A status pane displays the current status of LAN automation.
- Step 2** In the status pane, click **See Session Details**.
You can view the overall status of LAN Automation (In Progress or Completed), and also filter the view based on the discovered, or provisioned devices.
- Step 3** In the **LAN Automation** window, click **LAN Automated Devices** tab to see the configuration logs and session logs.
-

Create a Link Between Interfaces

To add a link between the interfaces through LAN Automation, follow these steps:

-
- Step 1** Click the menu icon (☰) and choose **Provision > LAN Automation**.
- Step 2** In the **LAN Automation Devices** tab of the **LAN Automation** window, click **Add Link**.
- Step 3** Follow these steps in the **Add Link** workflow:
- Select the two devices to establish the link.
 - Select an IP address pool within the LAN. Ensure that the IP address pool is reachable from Cisco DNA Center.
 - Select the interfaces on both the devices between which you want to establish a connection.
 - Click **Now** or **Later** to indicate when you want to provision the link. Enter a name for the task in the field provided.
 - In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
 - Click **Start Add Link**.

The **Link Configuration Started Successfully** window appears.

Step 4 To see the status of the configuration, click **View Status in Activities**.

Delete a Link Between Interfaces

To delete the interface links that were created during LAN Automation or by performing an Add Link operation, follow these steps:

Step 1 Click the menu icon (☰) and choose **Provision > LAN Automation**.

Step 2 In the **LAN Automation Devices** tab of the **LAN Automation** window, click **Delete Link**.

Step 3 Follow the steps in the **Delete Link** workflow:

- a) Select the two devices to delete the interface link.
- b) Select the interfaces on both these devices between which you want to delete the link.
- c) Click **Now** or **Later** to indicate when you want to start the delete process. Enter a name for the task in the field provided.
- d) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
- e) Click **Start Delete Link**.

The **LAN Automation configuration has been removed from the selected interfaces** window appears.

Step 4 To see the status of the delete link task, click **View Status in Activities**.



CHAPTER 21

Provision Fabric Networks

- [Cisco SD-Access Zero-Trust Security Solution, on page 463](#)
- [About Fabric Networks, on page 470](#)
- [New Automation for SD-Access, on page 472](#)
- [Add a Fabric Site, on page 473](#)
- [Configure Devices for a Fabric Site, on page 474](#)
- [Add a Device to a Fabric, on page 475](#)
- [Add a Device as a Border Node, on page 476](#)
- [Configure LISP Pub/Sub, on page 479](#)
- [Create an IP Transit, on page 480](#)
- [Create an SD-Access Transit, on page 480](#)
- [Select an Authentication Template, on page 481](#)
- [Configure Ports Within the Fabric Site, on page 482](#)
- [Configure Wireless SSIDs for Fabric Networks, on page 483](#)
- [Virtual Networks, on page 484](#)
- [Configure a Fabric Zone, on page 490](#)
- [Configure an Extended Node Device, on page 496](#)
- [Configure Supplicant-Based Extended Nodes, on page 502](#)
- [Configure a Port Channel, on page 509](#)
- [Multicast, on page 510](#)

Cisco SD-Access Zero-Trust Security Solution

Networks need protection against external and internal threats. Cisco SD-Access provides a zero-trust security solution for your workplace. The Cisco SD-Access zero-trust security solution provides secure access to users and devices from all locations across the network.

The Cisco SD-Access zero-trust security solution includes the following capabilities:

- **Identify and verify all endpoints:** SD-Access establishes an initial level of trust with each connecting endpoint.
- **Establish policy and segmentation:** SD-Access ensures least-privilege access based on the endpoint and user type.
- **Continuously monitor endpoints:** SD-Access continuously monitors the endpoints to ensure compliance.

- Threat mitigation: SD-Access allows you to quarantine the endpoints that are noncompliant or exhibit malicious behavior.

The Cisco SD-Access zero-trust security solution provides the flexibility to adopt a path to a zero-trust workplace based on your network settings and services. You can configure how users connect to the network using dynamic rules and automated segmentation.

The Cisco SD-Access zero-trust security solution provides the capability to automate network access policies using the following features:

- Endpoint visibility: You can identify and group endpoints. You can map their interactions through traffic flow analysis and define access policies.
- Trust monitoring: You can continuously monitor the endpoint behavior, scan for vulnerabilities, verify trustworthiness for continued access, and isolate rogue or compromised endpoints.
- Network Segmentation: You can enforce group-based access policies and secure network through multilevel segmentation.

The Cisco SD-Access zero-trust security solution enables you to explore various paths to zero-trust workplace based on your network settings and services. You can discover your optimal path based on your current network status, and explore the benefits of each added step on the zero-trust journey.

Zero-Trust Overview Dashboard

The SD-Access **Zero-Trust Overview** dashboard provides an overview of your zero-trust workplace journey. Click the menu icon (☰) and choose **Provision > Zero-Trust Overview** to view this dashboard.

The zero-trust workplace journey has the following phases:

- Day 0: For starting your zero-trust workplace journey. For more information, see [Day 0 View of Zero-Trust Overview Dashboard, on page 464](#).
- Day *n*: For ongoing monitoring and configuration changes of your zero-trust workplace journey. For more information, see [Day n View of Zero-Trust Overview Dashboard, on page 467](#).

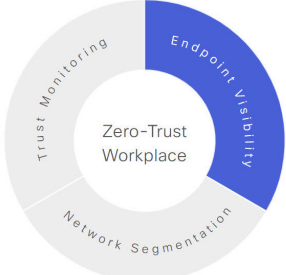
Day 0 View of Zero-Trust Overview Dashboard

Before you start your SD-Access zero-trust workplace journey, the day 0 view of the **Zero-Trust Overview** dashboard consists of the following sections:

Cisco DNA Center Provision / SD-Access / Zero-Trust Overview


Welcome to Cisco SD-Access! [Take a Tour](#)

SD-Access offers a turnkey, zero-trust security solution to automate network access policies. Security is deeply embedded within the network, and a software-defined approach allows rapid iteration and innovation.



Endpoint Visibility

Identify and group endpoints. Map their interactions through traffic flow analysis and define access policies.



Explore and start your journey to SD-Access Zero-Trust Workplace

Explore different paths to Zero-Trust Workplace based on your network settings and services. Flexible adoption pathways to reach complete SD-Access mean there is no one-user-fits-all approach. Discover your optimal path based on where your network is currently, and explore the benefits of each added step on on your Zero-Trust journey.

NETWORK CONNECTIVITY

[With Wireless](#) [With CAT9K](#) [With Traffic Telemetry Appliance](#)

SERVICES

[With ISE](#) [With Talos](#) [With CBAR Enabled](#)




I'm Done Exploring and Ready to Start My Journey

Once you are done exploring your options and have selected your preferred path settings above, click on Start My Journey to start your Cisco SD-Access to Zero-Trust Workplace.

Start my journey with creation of network fabric

I already have connectivity and want to start with Endpoint Visibility

[Start My Journey](#)



- **Welcome to Cisco SD-Access!:** This section consists of an overview video that provides a short overview of the multiple paths towards a full SD-Access zero-trust workplace. It also consists of a circle containing sections for each pillar of the SD-Access zero-trust workplace:
 - **Endpoint Visibility**
 - **Trust Monitoring**
 - **Network Segmentation**

Hover your cursor over each section to view more information.

- **Explore and start your journey to SD-Access Zero-Trust Workplace:** This section allows you to explore the different paths to a zero-trust workplace based on your network settings and services, and discover the optimal path for your network. This section consists of the **Network Connectivity** and **Services** options, and a circular journey map with details about the paths. Based on the options that you choose for network connectivity and services, the journey map displays the available paths to your zero-trust workplace journey.

To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

- **I'm Done Exploring and Ready to Start My Journey:** After exploring the paths and selecting your preferred settings, use this section to start your journey to a zero-trust workplace.

Get Started with SD-Access Zero-Trust Workplace Journey

Step 1 Click the menu icon (☰) and choose **Provision > Zero-Trust Overview**.

Step 2 Under **Explore and start your journey to SD-Access Zero-Trust Workplace**, do the following:

a) For **Network Connectivity** settings, choose the required options:

- Enable **With Wireless** to use wireless devices in your zero-trust workplace journey.
- Enable **With CAT9K** to use Cisco Catalyst 9000 Series devices or enable **With Traffic Telemetry Appliance** to use the Cisco DNA Traffic Telemetry Appliance in your zero-trust workplace journey.

b) For **Services** settings, choose the required options:

- Enable **With ISE** to use Cisco Identity Services Engine in your zero-trust workplace journey.
- Enable **With Talos** to use Talos Intelligence in your zero-trust workplace journey.
- Enable **With CBAR Enabled** to use Controller-Based Application Recognition (CBAR) in your zero-trust workplace journey.

c) (Optional) To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

Step 3 Under **I'm Done Exploring and Ready to Start My Journey**, choose one of the following options:

- To create a fabric network and start your journey towards a zero-trust workplace, click **Start my journey with creation of network fabric**.

- If you already have fabric network connectivity and want to start your journey towards zero-trust workplace with endpoint visibility, click **I already have connectivity and want to start with Endpoint Visibility**.

Step 4 Click **Start My Journey**.

Step 5 In the **Modify Journey Map** dialog box, do the following:

a) Review your journey map settings.

Note

- Cisco DNA Center displays a message if it doesn't discover the selected services for your network.
- Cisco DNA Center displays a message if it discovers additional services that were not selected in the journey.

b) (Optional) To remove a selected service from your journey map settings, uncheck the corresponding check box.

c) Click **Confirm**.

Day *n* View of Zero-Trust Overview Dashboard

After starting your SD-Access zero-trust workplace journey, the day *n* view of the **Zero-Trust Overview** dashboard consists of the following sections:

Cisco DNA Center Provision / SD-Access / Zero-Trust Overview

Your Journey to SD-Access Zero-Trust Workplace

Take a Tour

Zero Trust Workplace

Your journey to Zero-Trust Workplace

50%

Recommended Steps 1 of 3 ● Current Step

L2 Switched Access

SD-Access can be deployed alongside existing Layer 2 switched access networks, without prior conversion to Layer 3 routed access.

Tip

ROI Report 1 Month

---	---
TIME SAVED	COST SAVED

Your Journey Map

Modify My Journey Hide Map

⚠ Three (3) Warning Alerts on this page. [Expand](#) to see detail.

▼ Your Services and Network Settings SUGGESTED STEPS

- Wireless
- CAT9K
- Talos
- CBAR

Your SD-Access Overview

Virtual Networks

16

Virtual Networks

[Go to Page](#)

Fabric Sites

A portion of the fabric with its own control plane nodes, border nodes, and edge nodes.



[Go to Page](#)

Endpoint Analytics



Identify, verify, and build detailed endpoint profiles, and group similar endpoints by applying AI/ML techniques to better identify who/what is in the network.


[Go to Page](#)

- **Your Journey to SD-Access Zero-Trust Workplace:** This section consists of the following dashlets:
 - The **Zero Trust Workplace** dashlet displays the percentage progress of your zero-trust workplace journey.

- The **Recommended Steps** dashlet displays the next recommended steps for your zero-trust workplace journey. Use the arrow buttons ( and ) to scroll through all the steps. This dashlet also displays the tips for some steps. If available, click **Tip** to view the tips for the corresponding step.
- The **ROI Report** dashlet displays the time and cost savings based on the implemented steps as you progress through your zero-trust workplace journey. Use the drop-down in this dashlet to choose the time period for the report. Click **ROI Report** to view the report.
- **Your Journey Map**: This section displays the details of network connectivity and service settings for your zero-trust workplace journey. Click **Modify My Journey** to modify your zero-trust workplace journey. Click **Hide Map** to hide the journey map.

This section displays the warning alerts for your journey, if available. Click **Expand** to view the details of the alerts. If a selected service is currently unavailable in your network and you want to remove it from your journey, click the corresponding **Remove From Journey** option. If you want to get a selected service that is currently unavailable in your network, click the corresponding hyperlink to get the service.




Expand the **Your Services and Network Settings** drop-down to view the list of selected services for your journey. The  icon next to a service indicates that the service is currently available in your network. The  icon next to a service indicates that the service is currently unavailable in your network.

Hover your cursor over the corresponding  icon to view the **Update Needed** dialog box with details about the unavailable service. In the **Update Needed** dialog box, do the following:

- To remove the service from your journey, click **Remove From Journey**.
- To get the unavailable service in your network, click the corresponding hyperlink.


Enable the **Suggested Steps** toggle button to view the suggested order of steps around your journey map.

To view details about each step in the journey map, hover your cursor over the corresponding step around the journey map.

The  icon next to a step indicates that the corresponding configurations are incomplete. A number next to a step (for example, ) indicates the suggested order of the recommended steps for your journey map. The  icon next to a step indicates that the corresponding configurations are complete.

- **Your SD-Access Overview**: This section consists of dashlets for each functional area of your zero-trust workplace journey. Click the corresponding **Go to Page** option to open the relevant window. Each dashlet indicates its corresponding pillar of the zero-trust workplace journey in its upper-right corner.

Modify SD-Access Zero-Trust Workplace Journey

Step 1 Click the menu icon () and choose **Provision > Zero-Trust Overview**.

Step 2 Under **Your Journey Map**, click **Modify My Journey**.

Step 3 Under **Explore and start your journey to SD-Access Zero-Trust Workplace**, do the following:

a) For **Network Connectivity** settings, choose the required options:

- Enable **With Wireless** to use wireless devices in your zero-trust workplace journey.

- Enable **With CAT9K** to use Cisco Catalyst 9000 Series devices or enable **With Traffic Telemetry Appliance** to use the Cisco DNA Traffic Telemetry Appliance in your zero-trust workplace journey.

b) For **Services** settings, choose the required options:

- Enable **With ISE** to use Cisco Identity Services Engine in your zero-trust workplace journey.
- Enable **With Talos** to use Talos Intelligence in your zero-trust workplace journey.
- Enable **With CBAR Enabled** to use Controller-Based Application Recognition (CBAR) in your zero-trust workplace journey.

c) (Optional) To view details about each recommended step in the journey map, hover your cursor over the corresponding step around the journey map.

Step 4 Under **I'm Done Exploring and Ready to Start My Journey**, choose one of the following options:

- To create a fabric network and start your journey towards a zero-trust workplace, click **Start my journey with creation of network fabric**.
- If you already have fabric network connectivity and want to start your journey towards zero-trust workplace with endpoint visibility, click **I already have connectivity and want to start with Endpoint Visibility**.

Step 5 Click **Modify My Journey**.

Step 6 In the **Modify Journey Map** dialog box, do the following:

a) Review your journey map settings.

- Note**
- Cisco DNA Center displays a message if it doesn't discover the selected services for your network.
 - Cisco DNA Center displays a message if it discovers additional services that were not selected in the journey.

b) (Optional) To remove a selected service from your journey map settings, uncheck the corresponding check box.

c) Click **Confirm**.

About Fabric Networks

A fabric network is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric network in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.

Cisco DNA Center allows you to add devices to a fabric network. These devices can be configured to act as control plane, border, or edge devices within the fabric network.

Fabric Sites

A fabric site is an independent fabric area with a unique set of network devices: control plane, border, edge, wireless controller, ISE PSN. Different levels of redundancy and scale can be designed per site by including local resources: DHCP, AAA, DNS, Internet, and so on.

A fabric site can cover a single physical location, multiple locations, or only a subset of a location:

- Single location: branch, campus, or metro campus
- Multiple locations: metro campus + multiple branches
- Subset of a location: building or area within a campus

A Software-Defined Access fabric network may comprise multiple sites. Each site has the benefits of scale, resiliency, survivability, and mobility. The overall aggregation of fabric sites accommodates a large number of endpoints and scales modularly or horizontally. Multiple fabric sites are interconnected using a transit.

Transits

A transit is a site that interconnects two or more fabric sites or connects the fabric site with external networks (Internet, data center, and so on). There are two types of transit networks:

- IP transit: Uses a regular IP network to connect to an external network or to connect two or more fabric sites. It leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.
- SD-Access transit: Uses LISP/VxLAN encapsulation to connect two fabric sites. The SD-Access transit area may be defined as a portion of the fabric that has its own control plane nodes, but does not have edge or border nodes. However, it can work with a fabric that has an external border. With an SD-Access transit, an end-to-end policy plane is maintained using SGT group tags.

Fabric Readiness and Compliance Checks

Fabric Readiness Checks

Fabric readiness checks are a set of preprovisioning checks done on a device to ensure that the device is ready to be added to the fabric. Fabric readiness checks are now done automatically when the device is provisioned. Interface VLAN and Multi VRF configuration checks are not done as part of fabric readiness checks.

Fabric readiness checks include the following:

- Connectivity checks: Checks for the necessary connectivity between devices; for example, connectivity from the edge node to map server, from edge node to border, and so on.
- Existing configuration check: Checks for any configuration on the device that conflicts with the configuration that is pushed through SD-Access and can result in a failure later.
- Hardware version: Checks if the hardware version of the device is supported.
- Image type: Checks if the device is running with a supported image type (IOS-XE, IOS, NXOS, Cisco Controller).
- Loopback interface: Checks for the loopback interface configuration on the device. A device must have a loopback interface numbered 0 with an IP address configured on it to work with the SDA application.

Lack of a loopback interface numbered 0 may cause fabric provisioning errors because Loopback0 is used as the routing locator (RLOC) by default.

- Software license: Checks if the device is running with an appropriate software license.
- Software version: Checks if the device is running with an appropriate software image.

For more information on the software versions supported, see the [Cisco SD-Access Hardware and Software Compatibility Matrix](#).

If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. You can correct the problem and continue with the provisioning workflow for the device.

Fabric Compliance Checks

Fabric compliance is a state of a device to operate according to the user intent configured during the fabric provisioning. Fabric compliance checks are triggered based on the following:

- Every 24 hours for wired devices and every six hours for wireless devices.
- When there is a configuration change on the wired device.

A configuration change on the wired device triggers an SNMP trap, which in turn triggers the compliance check. Ensure that you have configured the Cisco DNA Center server as an SNMP server.

The following compliance checks are done to ensure that the device is fabric compliant:

- Virtual Network: Checks whether the necessary VRFs are configured on the device to comply with the current state of user intent for the VN on Cisco DNA Center.
- Fabric Role: Checks whether the configuration on the device is compliant with the user intent for a fabric role on Cisco DNA Center.
- Segment: Checks the VLAN and SVI configuration for segments.
- Port Assignment: Checks the interface configuration for VLAN and Authentication profile.

New Automation for SD-Access

The enhanced Cisco SD-Access user interface (UX) integrates simplicity, flexibility, and a rich, intuitive context. The Beta version of the Cisco SD-Access UX augments the user experience and provides the following capabilities:

- Greater clarity in the association between the fabric elements like virtual networks and fabric site
- Enhanced workflows
- Succinct view of the fabric elements and their attributes

The enhanced Cisco SD-Access UX consists of the following:

- A summary page, each for virtual networks, fabric sites, and transit networks
- The **Virtual Networks** Summary view has four sections:

- The first section displays a count of tasks at different stages, a count of Layer 3 virtual networks and anycast gateways, a count of anycast gateways, Layer 2 virtual networks and their VLANs.
 - The second section shows a graphical representation of the virtual network tasks.
 - The third section displays a list of the saved tips.
 - The final section displays a card-based view of the different workflows offered.
- The **Fabric Sites** page provides three views: Summary view, Map view, and Table view. The Summary view shows tips and insights, and workflows that are in progress. It also provides a summary of the number of fabric sites, fabric zones, fabric devices, control planes, and border nodes.
 - The **Transits** page displays a summary of the number of SD-Access transits, SDWAN transits, and IP-based transits. This page also gives you the option to create a transit network.

Use the **Preview New SD-Access** toggle button on the Cisco DNA Center menu bar to switch between the old and enhanced Cisco SD-Access UX.



Note All the tasks described in this chapter pertain to the enhanced Cisco SD-Access UX.

Add a Fabric Site

Before you begin

You can create a fabric site only if IP Device Tracking (IPDT) is already configured for the site.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of the fabric sites.
- Step 3** Click **Create Fabric Sites and Fabric Zones**.
- Alternatively, instead of the first three steps, click the menu icon (☰) and choose **Workflow > Create Fabric Sites and Fabric Zones**.
- Step 4** In the **Create Fabric Sites and Fabric Zones** window, click **Let's Do it** to go directly to the workflow.
- Step 5** In the **Fabric Site Location** window, choose an area, building, or floor to add as a fabric site.
- Step 6** In the **Wired Endpoint Data Collection** window, ensure that the **Wired Endpoint Data Collection** check box is checked.
- Step 7** In the **Authentication Template** window, do the following:
- a) Choose an authentication template for the fabric site:
 - **Closed Authentication:** Any traffic before authentication is dropped, including DHCP, DNS, and ARP.
 - **Open Authentication:** A host is allowed network access without having to go through 802.1X authentication.
 - **Low Impact:** Security is added by applying an ACL to the switch port, to allow very limited network access before authentication. After a host has been successfully authenticated, additional network access is granted.

- **None**
- b) (Optional) If you choose **Closed Authentication**, **Open Authentication**, or **Low Impact**, click **Edit** to edit the authentication settings:
- **First Authentication Method**: Choose **802.1x** or **MAC Authentication Bypass (MAB)**
 - **802.1x Timeout (in seconds)**: Use the slider to specify the 802.1x timeout, in seconds.
 - **Wake on LAN**: Choose **Yes** or **No**.
 - **Number of Hosts**: Choose **Unlimited** or **Single**.
 - **BPDU Guard**: Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.
 - **Pre-Authentication Access Control List**: Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action and enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

Step 8 In the **Fabric Zones** window, choose one of the following options:

- To designate fabric zones later, click **Setup Fabric Zones Later**.
- To designate fabric zones and create scoped subnets, click **Setup Fabric Zones Now** and choose a fabric site from the network hierarchy displayed.

Step 9 In the **Summary** window, review the fabric site settings.

You can edit any of the fabric site or zone settings here.

Step 10 Click **Deploy**.

It takes a few seconds for the site and zones to be provisioned. Upon successful creation of the site, a **Success! Your fabric site is created** message is displayed.

Configure Devices for a Fabric Site

You can configure the devices for a fabric site by using the following tabs:

- **Fabric Infrastructure**: Assign devices to fabric roles.
- **Authentication Template**: Select an authentication template for the fabric. An authentication template is a predefined set of configurations that are retrieved from Cisco ISE.
- **Wireless SSIDs**: Specify wireless SSIDs within the network that hosts can access. You can select the guest or enterprise SSIDs and assign address pools.
- **Port Assignment**: Apply specific configurations to each port, depending on the type of device that connects to the fabric site. To do this, select the ports that need a specific assignment, click **Assign**, and choose the port type from the drop-down list.

Note the following constraints:

- Cisco SD-Access deployments support only APs, extended nodes, user devices (such as a single computer or a single computer plus phone), and devices that need trunk ports such as single servers.
- Servers with internal switches or virtual switches aren't supported.
- Other networking equipment (such as hubs, routers, or switches) isn't supported.

Add a Device to a Fabric

After you have created a fabric site, you can add devices to the fabric site. You can also specify whether the device should act as a control plane node, an edge node, or a border node.

You can add a new device to the fabric site only if IP Device Tracking (IPDT) is configured for the fabric site.

A device which is assigned the Access role and has been provisioned before enabling IPDT on the site can't be added to the fabric. Reprovision such devices before adding them to the fabric site. Check the Provision workflow to confirm the status of **Deployment of IPDT** on the device.



Note

- It's optional to designate the devices in a fabric site as control plane nodes or border nodes. You might have devices that don't occupy these roles. However, every fabric site must have at least one control plane node device and one border node device. In the current release for wired fabric, you can add up to six control plane nodes for redundancy.
 - Currently, the Cisco Wireless Controller communicates only with two control plane nodes.
-

Before you begin

Provision the device if you haven't already provisioned it:

- The **Provision > Network Devices > Inventory** window displays the discovered devices.
- The topology view shows a device in gray color if it has passed the fabric readiness checks and is ready to be provisioned.
- If an error is detected during any of the fabric readiness checks, an error notification is displayed on the topology area. Click **See more details** to check the problem area listed in the resulting window. Correct the problem and click **Re-check** to ensure that the problem is resolved.
- If you update the device configuration as part of problem resolution, ensure that you resynchronize the device information by performing an **Inventory > Resync** for the device.



Note

You can continue to provision a device that has failed the fabric readiness checks.

Step 1 Click the menu icon (☰) and choose **Provision > Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Select the fabric site to add a device.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

Step 4 From the **List** view under the **Fabric Infrastructure** tab, click a device. A slide-in pane displays the following **Fabric** options:

Option	Description
Edge Node	Toggle the button next to this option to enable the selected device as an edge node.
Border Node	Toggle the button next to this option to enable the selected device as a border node.
Control Plane Node	Toggle the button next to this option to enable the selected device as a control plane node.

To configure a device as a fabric-in-a-box, select the **Control Plane Node**, **Border Node**, and **Edge Node** options.

To configure the device as a control plane and a border node, select both **Control Plane Node** and **Border Node**.

Step 5 Click **Add**.

What to do next

After a device is added to the fabric, fabric compliance checks are automatically performed to ensure that the device is fabric-compliant. The topology displays a device that has failed the fabric compliance check in blue color with a cross-mark beside it. Click **See more details** on the error notification to identify the problem area and correct it.

Add a Device as a Border Node

When you add a device to a fabric, you can add it in various combinations to act as a control plane node, border node, or edge node, as described in [Add a Device to a Fabric, on page 475](#).

This section describes how to add a device as a border node and configure the following:

- Border node type: Internal, External, or Internal and External ([Step 9, on page 477](#))
- Border node Priority ([Step 10, on page 477](#))
- Border node Affinity-ID ([Step 10, on page 477](#))
- Associated transit: SD-Access transit or IP-based transit ([Step 11, on page 478](#))
- IP address pool allocation for Layer 3 handoff ([Step 11, on page 478](#))

Before you begin

To use the Border Node Affinity-ID feature, ensure that you create an SD-Access LISP Pub/Sub transit. For more information, see [Create an SD-Access Transit, on page 480](#). When adding the first control plane node in the local fabric site, ensure that you select the LISP Pub/Sub control plane protocol. For more information, see [Configure LISP Pub/Sub, on page 479](#). The border node must be running Cisco IOS XE Release 17.8.1 or later.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** In the **Fabric Sites** tab, under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** In the **Fabric Sites** window, select the fabric site to configure a border node.
The resulting topology view displays all the devices in the network inventory. In the topology view, any device that is operating in a fabric role is shown in blue.
- Step 4** Under the **Fabric Infrastructure** tab, click a device.
- Step 5** In the slide-in pane, enable the **Border Node** toggle button.
- Step 6** In the resulting slide-in pane, click the **Layer 3 Handoff** tab.
- Step 7** Check the **Enable Layer 3 Handoff** check box.
- Step 8** Enter the **Local Autonomous Number** for the device.

If the local autonomous number is already configured on the device, this field displays the configured number and is disabled. You cannot change the local autonomous number if it's already configured on the device.
- Step 9** Configure the type of border node. By default, a border node is designated as an external border node, wherein it acts as the default gateway to the fabric site, without importing any external routes.

A border node can be configured to be an internal border node, wherein it isn't the default gateway and only imports external routes. A border node can also have a combined role of internal and external borders.
- Check both the **Default to all virtual networks** and **Do not import external routes** check boxes to designate the border as an external border node.
 - Uncheck both the **Default to all virtual networks** and **Do not import external routes** check boxes to designate the border as an internal border node.
 - Check the **Default to all virtual networks** check box to designate the border node as an external and internal border. It acts as the fabric default gateway and also imports BGP-learned routes into the fabric site. (Don't check the **Do not import external routes** check box.)
- For information about border node types, see the [Cisco SD-Access Solution Design Guide](#).
- Step 10** To configure the border node priority, affinity-ID and native multicast across SD-Access transit, click **Advanced Attributes** and configure the following:
- a) To change the border node priority, check the **Modify Border Priority** check box and enter a new priority value.
 - Priority value ranges from 1 to 10.
 - 1 indicates the highest priority.
 - 10 indicates the lowest priority.
 - The default priority value is 10.

If two or more border nodes are configured in a fabric site, traffic is routed through the border node that has a higher priority. If the priority values are the same, traffic is load balanced across the border nodes.
 - b) (Optional) To configure the border node affinity-ID, check the **Modify Border Node Affinity-ID** check box and enter values for the following fields:
 - **Affinity-ID Prime**: A lower relative prime value indicates a higher preference.

- **Affinity-ID Decider:** When the prime value is the same for two border nodes, the decider value is used as a tie-breaker to determine the border node preference.

Affinity-ID is a relative value, considering the value of this border node among the received values from all the other available border nodes. The lower the relative value of affinity-ID, the higher the preference for a destination border node. By default, the affinity-ID value isn't provisioned.

When the received affinity-ID values are equal, priority is used to determine the border node preference.

Note For proper functionality of the Affinity-ID feature, ensure that you configure an affinity-ID on all border nodes connected to the same SD-Access transit.

- c) (Optional) To configure native multicast over multiple sites that are connected to an SD-Access transit, check the **Enable Multicast over SD-Access Transit** check box.

Note Ensure that you enable a similar check box for the SD-Access transit too.

You can view the border node priority and affinity-ID deployment logs in **Activities > Audit Logs**.

Step 11

Hover your cursor over **Add Transit Site** and select a transit that will be connected to this border node.

In an **IP:BGP IP TRANSIT**, you can choose to either automate the IP address allocation for a virtual network or manually assign the Local and Peer IP addresses for a virtual network. You cannot do both.

- a) (Optional) To enable Cisco DNA Center to allocate IP address for the connection between the border node and peer, choose an IP address pool from the **Select IP Address Pool** drop-down list.

Note **Select IP Address Pool** is disabled if you have manually assigned the Local and Peer IP addresses.

- b) To configure the handoff interface, click **Add External Interface**.

Do the following steps in the resulting window:

1. Select an interface from the **External Interface** drop-down.
2. The **Remote AS Number** is automatically derived from the selected Transit or Peer network.
3. (Optional) Enter the a description for the interface in the **Interface Description** field.
4. (Optional) From the **Actions** drop-down list, choose **Enable All** or **Disable All**.
5. Click the **Enable Layer 3 Handoff** toggle button for the virtual network. This virtual network is advertised by the border node to the peer through BGP. You can select one, multiple, or all virtual networks.
6. In the **VLAN ID** field, enter an ID for the selected virtual network.
7. (Optional) To manually assign the IPv4 and IPv6 **Local IP Address** and **Peer IP Address** for the selected virtual network, enter the IP addresses and subnet mask in the CIDR notation (IP address/prefix-length).

Note The **Local IP Address** and **Peer IP Address** fields are disabled if you have already selected an IP Pool.

8. Click **Save**.

- c) Click **Add**.

Step 12

(Optional) Perform this step only if you are connecting a traditional network to the fabric site or you are migrating from a traditional network to an SD-Access network. Click the **Layer 2 Handoff** tab.

A list of virtual networks and the count of IP address pools in each virtual network is displayed.

- a) Click a virtual network that is to be handed off.

A list of IP address pools that are present in the virtual network and a list of interfaces through which you can connect to the traditional network are displayed.

- b) Select an interface from the **External Interface** drop down.
- c) (Optional) Enter a description for the interface in the **Interface Description** window.
- d) In the **External VLAN** field, enter the VLAN number into which the fabric must be extended.

A virtual network can be handed off on a single interface or on multiple interfaces. Layer 2 handoff for a segment can also be done on two different devices. In both cases, ensure that no loops are formed in the network.

Because a border node is connected to the traditional network, it is subject to broadcast storms, Layer 2 loops, and spanning-tree problems that can occur in Layer 2 switched access networks. To prevent disruption of control plane node services or border node services connecting to other external networks, a border node should be dedicated to the Layer 2 handoff feature and not colocated with other fabric roles or services.

- e) Click **Save**.

Step 13 Click **Add**.

Configure LISP Pub/Sub

You can configure LISP Pub/Sub on a fabric site only when you add the first control plane to your fabric.

Before you begin

Ensure that the fabric devices operate on Cisco IOS XE Release 17.6.1 or later.

Step 1 Click the menu icon (☰) and choose **Provision > Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Select the fabric site to add a device.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

Step 4 From the **List** view under the **Fabric Infrastructure** tab, click a device that is to be configured as a control plane.

Step 5 In the slide-in pane, enable the **Control Plane Node** toggle button to configure this plane.

Step 6 In the **Configure Control Plane** slide-in pane, choose **LISP Pub/Sub** route distribution protocol and click **Add**.


Step 7 Click **Add**.

Step 8 Click **Deploy**.

Step 9 In the **Modify Fabric** window, schedule the operation and click **Apply**.


To verify the configuration of LISP Pub/Sub in the fabric site, see the LISP Pub/Sub status on the **SITE SUMMARY** window.

Create an IP Transit


- Step 1** Click the menu icon () and choose **Provision > Transits**.
 - Step 2** Click **Create Transit**.
 - Step 3** In the **Transit** slide-in pane, enter a name for the transit network.
 - Step 4** Choose **IP-Based**.
The routing protocol is set to BGP by default.
 - Step 5** Enter the Autonomous System Number (ASN) for the transit network.
 - Step 6** Click **Save**.
-

Create an SD-Access Transit

To add an SD-Access transit:

- Step 1** Click the menu icon () and choose **Provision > Transits**.
- Step 2** Click **Create Transit**.
- Step 3** In the **Transit** slide-in pane, enter a name for the transit.
- Step 4** Choose an SD-Access **Transit Type**.

To configure a transit for the fabric sites that don't have a LISP Pub/Sub control plane, choose **SD-Access (LISP/BGP)**.
To configure a transit for the fabric sites that have a LISP Pub/Sub control plane, choose **SD-Access (LISP Pub/Sub)**.
To share the **SD-Access (LISP Pub/Sub)** Transit with other Cisco DNA Center clusters, choose **Yes, Share**. Otherwise, choose **No, keep it local**.

Note The **Yes, Share** option is visible only if the **Multiple Cisco DNA Center** package is installed on all the Cisco DNA Center clusters.
- Step 5** Choose a **Transit Control Plane Node Site** from the drop-down list. Choose at least one transit map server.
- Step 6** Choose a **Transit Control Plane Node** for the transit network from the drop-down list.
- Step 7** (Optional) To configure an additional map server, click the plus icon () and repeat [Step 5, on page 480](#) and [Step 6, on page 480](#).
- Step 8** (Optional) To configure native multicast over the LISP Pub/Sub-based SD-Access transit, click **Advanced Attributes**.
In the **Advanced Attributes** slide-in pane, check the **Multicast Over SD-Access Transit** check box.
In the **Advanced Attributes** slide-in pane, click **Save**.

Note To complete the native multicast configuration over multiple sites that are connected to the SD-Access transit, ensure that you enable multicast over SD-Access transit on the border nodes.
- Step 9** Click **Save**.

After a transit is created, the **Transits** window displays the newly created transit and its attributes.

Note You can't add an **SD-Access (LISP Pub/Sub)** transit to a fabric site that uses LISP/BGP control plane. You can't add **SD-Access (LISP/BGP)** transit to a fabric site that uses LISP Pub/Sub control plane.

What to do next

To interconnect the fabric sites with an SD-Access Transit, add the transit to the border node.

Select an Authentication Template

You can configure an authentication template that applies to all devices in the fabric site.

Step 1 Click the menu icon (☰) and choose **Provision > Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Click a fabric site.

Step 4 Click the **Authentication Template** tab.

Step 5 Under **Select Authentication Template**, choose an authentication template for the site:

- **Open Authentication:** A host is allowed network access without having to go through 802.1X authentication.
- **Closed Authentication:** Any traffic prior to authentication is dropped, including DHCP, DNS, and ARP.
- **Low Impact:** Security is added by applying an ACL to the switch port, to allow limited network access prior to authentication. After a host has been successfully authenticated, additional network access is granted.
- **None**

You can edit the settings of the selected authentication template to address site-specific authentication requirements.

Before you change the site-level authentication, you must resynchronize any fabric device whose Access Points were onboarded through macros or autoconf and haven't yet undergone the periodic resync.

Step 6 (Optional) To edit the settings of the chosen authentication method, click **Edit**.

a) In the slide-in pane, complete the following:

- **First Authentication Method:** Choose **802.1x** or **MAC Authentication Bypass (MAB)**
- **802.1x Timeout (in seconds):** Use the slider to specify the 802.1x timeout, in seconds.
- **Wake on LAN:** Choose **Yes** or **No**.

Wake on LAN (WoL) is supported only in the following scenarios:

- The source (WoL initiator) and destination (sleeping host) are both in the same subnet and Layer 2 Flooding is enabled.
- The source is outside the SD-Access fabric but located in the network that is connected to the fabric through Layer 3 handoff and the destination is in an SD-Access subnet with IP-Directed Broadcast enabled.

- Note** The following topologies do not support Wake on LAN:
- The WoL initiator and the sleeping host are on different subnets within the same Layer 3 Virtual Network.
 - The WoL initiator routes to the sleeping host over an SD-Access Transit.
- **Number of Hosts:** Choose **Unlimited** or **Single**.
- Note** **Number of Hosts** specifies the number of data hosts that can be connected to a port. With **Single**, you can have only one data client on the port. With **Unlimited**, you can have multiple data clients and one voice client on the port.
- **Pre-Authentication Access Control List:** Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action. Enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

b) Click **Save**.


The saved modifications apply only to the site for which the authentication template is edited.

Step 7 Click **Deploy**.

The Hitless Authentication Change feature lets you switch from one authentication method to another without removing the devices from the fabric.

Configure Ports Within the Fabric Site

The **Port Assignment** tab lets you configure each access device in the fabric site. You can specify network behavior settings for each port on a device.

Step 1 Click the menu icon () and choose **Provision > Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Select a fabric site.

Step 4 Click the **Port Assignment** tab.

Step 5 From the list of fabric devices, expand the drop-down corresponding to the device that you want to configure. The ports that are available on the device are displayed.

Step 6 Check the corresponding check box.

Step 7 Hover your cursor over **Configure** and choose **Assign Ports**.

Step 8 In the slide-in pane, choose the **Connected Device Type**:

Option	Description
User Devices (ip-phone, computer, laptop)	Configures the port to connect to a host device.
Access Point (AP)	Configures the port to connect to an access point.
Trunk	Configure the port as a trunk port.

Option	Description
Supplicant-Based Extended Node	Configures the port to receive a supplicant-based extended node.

- To connect host devices, choose **User Devices (ip-phone, computer, laptop)** and do the following:
 - a. Choose the VLAN name for data from the **VLAN Name (Data)** drop-down list.
 - b. Choose a security group from the **Security Group** drop-down list.
Security groups are supported only with the **None** authentication template.
 - c. Choose the VLAN name for voice from the **VLAN Name (Voice)** drop-down list.
 - d. Choose the authentication type from the **Authentication Template** drop-down list.
 - e. Enter a **Description** for the connected device.
- To connect an access point, choose **Access Point (AP)** and do the following:
 - a. Choose the VLAN name from the **VLAN Name (Data)** drop-down list.
 - b. Choose the authentication type from the **Authentication Template** drop-down list.
 - c. Enter a **Description** for the connected device.
- To connect a supplicant-based extended node device, choose **Supplicant-Based Extended Node**.
- To connect a trunk port, choose **Trunk** and enter a **Description** for the port.

Step 9 Click **Update**.

Configure Wireless SSIDs for Fabric Networks

Before you begin

Ensure to add the wireless device to the fabric site.

- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** Select a fabric site.
- Step 4** Click the **Wireless SSIDs** tab and specify the wireless SSIDs within the network that the hosts can access.
- Step 5** From the **Choose Pool** drop-down list, choose an IP address pool reserved for the SSID.
The wireless IP address pools that are configured for Layer 3 and Layer 2 segments are available in this drop-down list.
- Step 6** From the **Assign SGT** drop-down list, choose a security group for the SSID.
- Step 7** Check the **Enable Wireless Multicast** check box to enable wireless multicast on the SSIDs.




Virtual Networks

Virtual networks are overlays that are used to segment traffic within a common physical network infrastructure; this is also known as macrosegmentation. Layer 2 virtual networks segment switched traffic, and Layer 3 virtual networks segment routed traffic. Each endpoint that is connected to a Cisco SD-Access fabric is assigned to a specific virtual network based on the static edge port configurations or the dynamic policy from the Cisco Identity Service Engine. Within a virtual network, endpoints can communicate with each other unless explicitly blocked by microsegmentation policy. Endpoints across different virtual networks cannot communicate with each other by default. Intervirtual network traffic requires connectivity policy to be implemented outside of the Cisco SD-Access fabric, such as on a fusion device.

A typical use case for virtual networks is an office building containing both corporate endpoints and building-management systems. The corporate endpoints must be segmented from building systems, such as lighting, heating, ventilation, and air conditioning. In such a scenario, a network administrator can use macrosegmentation to segment the corporate endpoints and the building systems using two or more virtual networks to block unauthorized access between the building systems and corporate endpoints.

A Layer 3 virtual network may span multiple fabric sites and across network domains (wireless LAN, campus LAN, and WAN). A Layer 2 virtual network resides within a single fabric site.

Create a Layer 3 Virtual Network


-
- Step 1** Click the menu icon () and choose **Workflows > Create Layer 3 Virtual Networks**. Alternatively, you can navigate to the **Layer 3** tab in **Provision > Virtual Networks** and click **Create Layer 3 Virtual Networks**.
- Step 2** If the task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 3** In the **Layer 3 Virtual Networks** window, do the following:
- In the **Layer 3 Virtual Network name** field, enter a name for the Layer 3 virtual network.
 - (Optional) To create another Layer 3 virtual network, click the plus icon () and enter a name for the Layer 3 virtual network.
- Step 4** In the **Fabric Sites and Fabric Zones (Optional)** window, configure the following:
- Click **Select Fabric Sites** and choose the fabric sites.
You can assign a virtual network to multiple fabric sites. To choose the fabric sites, do one of the following:
 - Click the plus icon () next to the required fabric sites.
 - Click the fabric site name and click **Add Selected**.

Note To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.

 - To choose all the fabric sites, click **Add All**.

Repeat this association for all the Layer 3 virtual networks that you created.

- Click **Assign**.
- Click **Select Fabric Zones** and do one of the following:

- Click the plus icon () next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.
Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.
- To choose all the fabric zones, click **Add All**.

d) Click **Assign**.

Step 5 Review the Layer 3 virtual network settings in the **Summary** window.


Step 6 In the **Created and Deploy (Step 1 of 2)** window, click **Create** to create the context of the virtual network.

Step 7 In the **Created and Deploy (Step 2 of 2)** window, click **Deploy** to assign the virtual network to the selected sites.

Step 8 To verify the virtual network creation, click **View Layer 3 Virtual Networks**.

In the **Virtual Networks** window, the **Layer 3** tab displays the details of all the Layer 3 virtual networks.

Create a Layer 2 Virtual Network

Step 1 Click the menu icon () and choose **Workflows > Create Layer 2 Virtual Networks**.


Alternatively, you can navigate to the **Layer 2** tab under **Provision > Virtual Networks** and click **Create Layer 2 Virtual Networks**.

Step 2 If the task overview window opens, click **Let's Do it** to go directly to the workflow.

Step 3 In the **Configuration Attributes** window, configure the following:


- a) In the **VLAN Name** field, enter the VLAN name.
- b) In the **VLAN ID** field, enter the VLAN ID. The valid range for VLAN ID is from 2 through 4093.

Note The VLAN IDs from 1002 through 1005 and 2046 are reserved VLAN IDs.

- c) From the **Traffic Type** area, choose **Data** or **Voice**.
- d) Check the **Fabric-Enabled Wireless** check box to enable wireless.
The **Layer 2 Flooding** check box is enabled by default for a Layer 2 virtual network.
- e) To add another Layer 2 virtual network, click the plus icon () and repeat [3.a, on page 485](#) to [3.d, on page 485](#).

Step 4 In the **Associated Fabric Sites and Fabric Zones** window, choose a fabric site for the Layer 2 virtual network from the **Fabric Sites** drop-down. Optionally, to choose the fabric zone to associate with this Layer 2 virtual network, do the following:

a) Click **Select Fabric Zones** and do one of the following:

- Click the plus icon () next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.
Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.
- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

Repeat this association for all the Layer 2 virtual networks that you created.


Step 5 In the **Summary** window, review your Layer 2 virtual network settings and click **Create**.

Step 6 In the **Create** window, click **Deploy** to deploy the Layer 2 virtual network.

After the Layer 2 virtual network is provisioned, a success message is displayed.

Step 7 To verify the virtual network creation, click **View Layer 2 Virtual Networks**. In the **Virtual Networks** window, the **Layer 2** tab displays the details of all the Layer 2 virtual networks.

Associate Layer 3 Virtual Networks to Fabric Sites

Step 1 Click the menu icon () and choose **Provision > Virtual Networks**.

Step 2 Under **SUMMARY**, click the number that indicates the count of **Layer 3 Virtual Networks**.

The resulting window displays all the Layer 3 virtual networks that are created at the global level.

Step 3 In the **Layer 3** tab, check the check box next to the Layer 3 virtual networks for which you want to edit the fabric site association.


Note You can edit up to five Layer 3 virtual networks.

Step 4 Hover your cursor over **More actions**, and choose **Edit Fabric Site and Fabric Zone Associations**.

Step 5 In the **Fabric Sites and Fabric Zones (Optional)** window, configure the following:

a) Click **Select Fabric Sites** and choose the fabric sites.

You can assign a virtual network to multiple fabric sites. To choose the fabric sites, do one of the following:

- Click the plus icon () next to the required fabric sites.
- Click the fabric site name and click **Add Selected**.


Note To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.

- To choose all the fabric sites, click **Add All**.

Repeat this association for all the Layer 3 virtual networks.

b) Click **Assign**.

c) Click **Select Fabric Zones** and do one of the following:

- Click the plus icon () next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

d) Click **Assign**.

- Step 6** Review the Layer 3 virtual network sites on the **Summary** window.
- Step 7** In the **Created and Deploy (Step 1 of 2)** window, click **Update** to assign the Layer 3 virtual networks to the selected sites.
- Step 8** In the **Created and Deploy (Step 2 of 2)** window, click **Deploy** to deploy the Layer 3 virtual networks.
- Step 9** To verify the virtual networks, click **View Layer 3 Virtual Networks**.
In the **Virtual Networks** window, the **Layer 3** tab displays the details of all the Layer 3 virtual networks.

Create Anycast Gateways

Before you begin

Ensure that you have created a Layer 3 virtual network. For more information, see [Create a Layer 3 Virtual Network, on page 484](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of **Anycast Gateways**.
- Step 3** In the **Anycast Gateway** tab, click **Create Anycast Gateways**.
Alternatively, click the menu icon and choose **Workflows > Create Anycast Gateways**.
- Step 4** If the task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 5** In the **Layer 3 Virtual Networks** window, select one or more virtual networks to add a gateway.
- Click the plus icon (+) next to the required fabric sites.
 - Click the fabric site name and click **Add Selected**.
- Note** To choose multiple fabric sites, press **Shift**, click the fabric site names, and click **Add Selected**.
- To choose all the fabric sites, click **Add All**.
- Step 6** In the left pane of the **Configuration Attributes** window, choose the Layer 3 virtual network for which you want to create the anycast gateway and do the following:
- a) From the **IP Address Pool** drop-down list, choose an IP address pool.
 - b) For **INFRA_VN**, do the following:
 - Choose **AP** or **Extended Node** from the **Pool Type** drop-down list.
 - Enter a valid **VLAN Name** or check the **Auto generate VLAN name** check box.
 - Enter a custom **VLAN ID** for the virtual network.
 - To onboard a supplicant-based extended node, check the **Supplicant-Based Extended Node Onboarding** check box.
- Note** This check box is active only when you choose the **Extended Node** pool type.

- c) To enable the IP-Directed Broadcast feature, check the **IP-Directed Broadcast** check box.

Note

- When you enable Directed Broadcast, Cisco DNA Center automatically enables Layer 2 flooding.
- Routers and Cisco Nexus 7000 Series Switches don't support Directed Broadcast.
- Before enabling Directed Broadcast, ensure that you have enabled underlay multicast.

- d) To enable the intrasubnet routing, check the **Intra-Subnet Routing** check box.

Note When you enable intrasubnet routing, Cisco DNA Center automatically disables the **Fabric-Enabled Wireless** and **Layer 2 Flooding** check boxes.

- e) Enter a valid **VLAN Name** or check the **Auto generate VLAN name** check box.

- f) Enter a custom **VLAN ID** for the virtual network.

Note

- VLAN IDs 1, 1002-1005, 2046, and 4095 are reserved and can't be used.
- If you don't provide a custom VLAN ID, Cisco DNA Center generates a VLAN ID in the range of 1021–2020.

- g) Choose **Data** or **Voice** from the **Traffic Type** area.

- h) From the **Security Group** drop-down list, choose a security group.

- i) To include this IP pool in the critical IP address pool, check the **Critical VLAN** check box.

A critical pool is used for closed authentication profile when an authentication server isn't available. A critical VLAN is assigned to the critical pool and all unauthenticated hosts are placed in the critical VLAN in the absence of an authentication server.

Note When you enable critical VLAN, Cisco DNA Center automatically generates the VLAN name.

- j) To enable this IP pool as a wireless IP address pool, check the **Fabric-Enabled Wireless** check box.

- k) To enable Layer 2 flooding, check the **Layer 2 Flooding** check box.

Note Layer 2 flooding requires underlay multicast, which is configured during LAN automation. If you don't provision the underlay through LAN automation, configure the underlay multicast manually.

- l) To enable onboarding of bridge-mode virtual machines that are connected to the fabric-enabled wireless network, check both the **Fabric Enabled Wireless** and the **Multiple IP to MAC** check boxes.

- m) To enable a wired host to have multiple IPv4 addresses (IP aliasing), check only the **Multiple IP to MAC** check box.

You can have a maximum of 1000 IPv4 addresses for a single MAC address.

- n) To associate more IP pools, click the plus icon (+) and repeat the steps.

Step 7

In the **Fabric Zones (Optional)** window, do the following:

- a) Click **Select Fabric Zones** and do one of the following:

- Click the plus icon (+) next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

b) Click **Assign**.

Step 8 Review the anycast gateway settings in the **Summary** window.

Step 9 In the **Create** window, click **Deploy**.

Step 10 To verify the gateway creation after you see a success message, click **View Anycast Gateway**.

In the **Virtual Networks** window, the **Anycast Gateway** tab displays the details of all the anycast gateways.

Virtual Network Policy

Configure a virtual network (VN) policy to allow route leaks between Layer 3 VNs, without using a fusion device. Use a VN policy to provide the endpoints (hosts or users) with access to shared services like DHCP, DNS, Internet access, and so on, through Cisco DNA Center automation. The shared services connect to a Provider VN. The endpoints that use the shared services reside in a Subscriber VN. A VN policy establishes communication between the Provider VN and the Subscriber VNs.

You can create a VN policy, edit a VN policy, and delete a VN policy for the following deployments:

- Single site fabric with IP Transit
- Multi-site fabric with SDA Transit

Guidelines to Configure a Virtual Network Policy

Consider the following guidelines before you configure a virtual network policy:

- To configure a VN Policy, a device should operate Cisco IOS XE 17.9.1 or a later release.
- VN Policy is supported only on the fabric sites that have a LISP Pub/Sub control plane.
- To configure a VN policy on a multisite fabric with SD-Access transit, ensure that all the sites have the provider VN.
- If you configure multiple VN policies in your network, the same VN cannot be the Provider VN in more than one policy.
- VN Policy does not support overlapping IP pools.
- Provider VN in a policy cannot be configured as a Subscriber VN in another VN Policy and conversely.
- Add the Provider VN to all the fabric sites where a VN Policy is applicable.
- Ensure that the Provider VNs do not leak into each other outside the fabric. Else, it might result in route leaks between the Subscriber VNs.
- VN policy is not supported on router devices.

Create a Virtual Network Policy

To create a VN policy, follow these steps:

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Create Virtual Network Policy**.
Alternatively, navigate to **Layer 3 Virtual Networks** tab under **Provision > Virtual Networks** and click **Policies**. In the **Policies** window, click **Create Virtual Network Policy**.
- Step 2** Follow the on-screen guidance to provide a name for the policy, to select a Provider VN and the Subscriber VNs.
You can assign this VN policy to one or more fabric sites.
In a multisite deployment where an SD-Access transit connects the fabric sites, ensure that you select all the fabric sites that are connected by the SD-Access transit.
- Step 3** On the **Summary** page, review the VN Policy configuration.
To make changes, click **Edit** next to the group of settings that you want to change.
- Step 4** Click **Create**.
-

Edit a Virtual Network Policy

You can edit a VN Policy to add or delete Subscriber VNs and to assign or remove the policy from a fabric site.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Click the number that indicates the count of **Layer 3 Virtual Networks**.
- Step 3** In the **Policies** tab, select the policy to be edited, and click **More Actions > Edit Policy**.
- Step 4** Follow the on-screen guidance to edit the policy.
-

Delete a Virtual Network Policy

To delete a VN Policy, follow these steps:

-
- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Click the number that indicates the count of **Layer 3 Virtual Networks**.
- Step 3** In the **Policies** tab, select the policy to be deleted, and click **More Actions > Delete Policy**.
- Step 4** In the **Delete Policy** slide-in pane, click **Apply**.
-

Configure a Fabric Zone

A fabric site (parent site) can be divided into fabric zones with smaller subnets to help you manage the network easily. A fabric zone can have its own edge nodes and extended nodes, but it connects to the parent site for a control plane and border. If you migrated from an earlier Cisco DNA Center release to the current release,

you can create a fabric zone on the existing fabric site. This fabric zone inherits all the properties of its parent site.

Before you begin

- Ensure that you have created a network hierarchy under the Global site.
- Select a parent site that is not at the lowest level in the hierarchy.

The following is the broad workflow to configure a fabric zone.

1. Create a fabric zone in one of the following ways:
 - Create a fabric site and its zones using the **Create Fabric Site** workflow. For more information, see [Create a Fabric Site and Its Fabric Zones, on page 491](#).
 - Edit an existing fabric site to add fabric zones to it. For more information, see [Create a Fabric Zone Within a Fabric Site, on page 492](#).
2. Add edge nodes and extended nodes to the fabric zone. For more information, see [Add a Device to a Fabric, on page 475](#).
3. Assign Layer 3 virtual networks and segments to the fabric zone. For more information, see [Associate Layer 3 Virtual Networks to Fabric Zones, on page 493](#).



Note Only the virtual networks and segments of the parent site are available to the fabric zone.



Note After a segment is added to a fabric zone, it can't be updated in the parent site.
You can't edit edge nodes and extended nodes of a fabric zone in its parent site.
You can configure the edge node of a fabric zone as a control plane or a border of the parent site.

Create a Fabric Site and Its Fabric Zones

Step 1 Click the menu icon (☰) and choose **Provision > Fabric Sites**.

Step 2 Click **Create Fabric Sites and Fabric Zones**.

Alternatively, click the menu icon and choose **Workflows > Create Fabric Sites and Fabric Zones**.

Step 3 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 4 In the **Fabric Site Location** window, choose an area, building, or floor to add as a fabric site.

Step 5 In the **Wired Endpoint Data Collection** window, ensure that the **Wired Endpoint Data Collection** check box is checked.

Step 6 In the **Authentication Template** window, do the following:

a) Choose an authentication template for the fabric site:

- **Closed Authentication:** Any traffic before authentication is dropped, including DHCP, DNS, and ARP.

- **Open Authentication:** A host is allowed network access without having to go through 802.1X authentication.
- **Low Impact:** Security is added by applying an ACL to the switch port, to allow limited network access before authentication. After a host has been successfully authenticated, additional network access is granted.
- **None**

b) (Optional) If you choose **Closed Authentication**, **Open Authentication**, or **Low Impact**, click **Edit** to edit the authentication settings:

- **First Authentication Method:** Choose **802.1x** or **MAC Authentication Bypass (MAB)**
- **802.1x Timeout (in seconds):** Use the slider to specify the 802.1x timeout, in seconds.
- **Wake on LAN:** Choose **Yes** or **No**.
- **Number of Hosts:** Choose **Unlimited** or **Single**.
- **BPDU Guard:** Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.
- **Pre-Authentication Access Control List:** Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action. Enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

Step 7 In the **Fabric Zones** window, to designate fabric zones and create scoped subnets, click **Setup Fabric Zones Now**.

To enable a fabric zone, choose a fabric site in the network hierarchy.

Step 8 In the **Summary** window, review the fabric site settings.

You can edit any of the fabric site or zone settings here.

Step 9 Click **Deploy**.

It takes a few seconds for the site and zones to be provisioned. Upon successful creation of the site, a success message is displayed.

The newly created fabric zone is tagged with an “FZ” in the site hierarchy pane.

Create a Fabric Zone Within a Fabric Site

Step 1 Click the menu icon (☰) and choose **Provision > Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 For the fabric site where you want to designate fabric zone, under the **Actions** column, hover your cursor over the ellipsis icon (⋮) and choose **Edit Fabric Zone**.

Step 4 In the **Fabric Zones** window, choose an area, building, or floor.

Step 5 Review the fabric site settings in the **Summary** window.

You can edit any of the fabric site or zone settings here.

Step 6 Click **Deploy**.

It takes several seconds for the fabric site and fabric zones to be provisioned. After the provisioning, a success message is displayed.

The newly created fabric zone is tagged with an “FZ” in the site hierarchy pane.

What to do next

- Add only edge node and extended node devices to the newly created fabric zone.
Devices assigned to a fabric zone can't be assigned to the parent site. However, an edge node device assigned to a fabric zone can still be configured as a control plane or a border node for the parent site.
- Assign IP pools and virtual networks to the fabric zone.

Associate Layer 3 Virtual Networks to Fabric Zones

Before you begin

Ensure that you have created the fabric zone.



Note You can add only the Layer 3 virtual networks of a parent site to a fabric zone.

Step 1 Click the menu icon (☰) and choose **Provision > Virtual Networks**.

Step 2 Under **SUMMARY**, click the number that indicates the count of **Layer 3 Virtual Networks**.

The resulting window displays all the Layer 3 virtual networks at a global level.

Step 3 In the **Layer 3** tab, check the check box next to the Layer 3 virtual networks for which you want to edit the fabric zone associations.

Note You can edit up to five Layer 3 virtual networks.

Step 4 Hover your cursor over **More actions**, and choose **Edit Fabric Site and Fabric Zone Associations**.

Step 5 In the **Fabric Sites and Fabric Zones (Optional)** window, configure the following:

a) Click **Select Fabric Zones** and choose the fabric zones.

You can assign a virtual network to multiple fabric zones in a fabric site. To choose the fabric zones, do one of the following:

- Click the plus icon (+) next to the required fabric zones.
- Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

- To choose all the fabric zones, click **Add All**.

- b) Click **Assign**.
- c) Repeat this association for all the Layer 3 virtual networks.

- Step 6** Review the Layer 3 virtual network zones on the **Summary** window.
- Step 7** In the **Created and Deploy (Step 1 of 2)** window, click **Update**.
- Step 8** In the **Created and Deploy (Step 2 of 2)** window, click **Deploy** to deploy the Layer 3 virtual networks.
- Step 9** To verify the virtual networks, click **View Layer 3 Virtual Networks**.
In the **Virtual Networks** window, the **Layer 3** tab displays the details of all the Layer 3 virtual networks.

Associate Layer 2 Virtual Networks to Fabric Zones

Before you begin



Note After you add the gateways to a fabric zone, you can't edit them at the parent site.

- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of **Layer 2 Virtual Networks**.
The resulting window displays all the Layer 2 virtual networks at a global level.
- Step 3** Click Fabric Site: **Global**.
- Step 4** In the **Select Fabric Site** slide-in pane, choose a fabric site and click **Select**.
- Step 5** In the **Layer 2** tab, check the check box next to the Layer 2 virtual networks for which you want to edit the fabric zone associations.
- Note** You can edit up to five Layer 2 virtual networks.
- Step 6** Hover your cursor over **More actions**, and choose **Edit Layer 2 Fabric Zone Associations**.
- Step 7** In the **Associated Fabric Sites and Fabric Zones** window, configure the following:
- a) Click **Select Fabric Zones** and choose the fabric zones.
You can assign a virtual network to multiple fabric zones in a fabric site. To choose the fabric zones, do one of the following:
 - Click the plus icon (+) next to the required fabric zones.
 - Click the fabric zone name and click **Add Selected**.

Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.

 - To choose all the fabric zones, click **Add All**.
 - b) Click **Assign**.
 - c) Repeat this association for all the Layer 2 virtual networks.

- Step 8** In the **Summary** window, review your Layer 2 virtual network settings and click **Create**.
- Step 9** In the **Create** window, click **Deploy** to deploy the Layer 2 virtual network.
After the Layer 2 virtual network is provisioned, a success message is displayed.
- Step 10** To verify the virtual network creation, click **View Layer 2 Virtual Networks**. In the **Virtual Networks** window, the **Layer 2** tab displays the details of all the Layer 2 virtual networks.

Associate Anycast Gateways to Fabric Zones

Before you begin

Ensure that you have created the fabric zone.



Note You can add only the anycast gateways of a parent site to a fabric zone.

After you add an anycast gateway to a fabric zone, you can't update it at the parent site.

- Step 1** Click the menu icon (☰) and choose **Provision > Virtual Networks**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of **Anycast Gateways**.
The resulting window displays all the anycast gateways at a global level.
- Step 3** Click Fabric Site: **Global**.
- Step 4** In the **Select Fabric Site** slide-in pane, choose a fabric site and click **Select**.
- Step 5** In the **Anycast Gateway** tab, check the check box next to the anycast gateways for which you want to edit the fabric zone associations.
- Note** You can edit up to five anycast gateways.
- Step 6** Hover your cursor over **More actions**, and choose **Edit Fabric Zone Associations**.
- Step 7** In the **Fabric Zones (Optional)** window, do the following:
- Click **Select Fabric Zones** and do one of the following:
 - Click the plus icon (+) next to the required fabric zones.
 - Click the fabric zone name and click **Add Selected**.
Note To choose multiple fabric zones, press **Shift**, click the fabric zone names, and click **Add Selected**.
 - To choose all the fabric zones, click **Add All**.
 - Click **Assign**.
- Step 8** Review the anycast gateway settings in the **Summary** window.
- Step 9** In the **Create** window, click **Deploy**.
- Step 10** To verify the gateway creation after you see a success message, click **View Anycast Gateway**.

In the **Virtual Networks** window, the **Anycast Gateway** tab displays the details of all the anycast gateways.

Configure an Extended Node Device

An extended node is configured by automated workflow. After configuration, the extended node device is displayed in the fabric topology view. You can assign ports for the extended nodes using the **Port Assignment** tab.



Note You can't onboard the extended nodes through the GUI-based provisioning workflows. An Extended node is onboarded only through the SD-Access automated workflow after resetting the device configuration to the factory default and powering on the device.

A device is onboarded according to the Cisco DNA license of its Extended Node neighbor and its own Cisco DNA license:

- If the neighbor is operating with a Cisco DNA Essentials license, the device is onboarded as a standard Extended Node, regardless of its Cisco DNA license.
- If the neighbor is operating with a Cisco DNA Advantage license, the device is onboarded as a standard Extended Node if it has a Cisco DNA Essentials license.
- If the neighbor is operating with a Cisco DNA Advantage license, the device is onboarded as a Policy Extended Node if it has a Cisco DNA Advantage license.
- If the device has more than one neighbor, and those neighbors have different Cisco DNA license levels, the device is onboarded as a standard Extended Node, regardless of its Cisco DNA license.

Extended node devices support multicast traffic.

Policy Extended Nodes are extended nodes that support security policy within the virtual network. You can select a **Group** during port assignment for a Policy Extended Node.

Policy Extended Node devices include Cisco Catalyst Industrial Ethernet (IE) 3400, IE 3400 Heavy Duty series switches, and Cisco Catalyst 9000 series switches that run Cisco IOS XE Release 17.1.1s or later.

Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches, and Cisco Industrial Ethernet 4000, 4010, and 5000 series switches can't be configured as Policy Extended Nodes.

Steps to Configure an Extended Node

When configured as a fabric edge, Cisco Catalyst 9300, Cisco Catalyst 9400, and Cisco Catalyst 9500 series switches support extended nodes.



Note Cisco Catalyst 9200 series switches that are configured as fabric edge nodes don't support extended node devices.

The following are the minimum supported software versions on the extended nodes:

- Cisco Industrial Ethernet 4000, 4010, 5000 series switches: 15.2(7)E0s with LAN base license enabled. If you have an IP services license, you must change the Switch Database Management (SDM) template to `dual-ipv4-and-ipv6 default` manually.
- Cisco Catalyst IE 3400, 3400 Heavy Duty (X-coded and D-coded) series switches: Cisco IOS XE Release 17.1.1s.
- Cisco Catalyst IE 3300 series switches: Cisco IOS XE Release 16.12.1s.
- Cisco Digital Building series switches, Cisco Catalyst 3560-CX switches: Release 15.2(7)E0s.

The minimum software version that is required on a policy extended node device and on the edge node device supporting the policy extended node is Cisco IOS XE Release 17.1.1s.


The following configuration steps are applicable to both a standard Extended Node and Policy Extended Node.

Before you begin

To configure a device as a Policy Extended Node, both the device and the edge node supporting it must have the Network Advantage and DNA Advantage license levels enabled.

-
- Step 1** Configure a network range for the extended node. See [Configure IP Address Pools, on page 202](#). This step comprises adding an IP address pool and reserving the IP pool at the site level. Ensure that the CLI and SNMP credentials are configured.
- Step 2** Assign the extended IP address pool to INFRA_VN. See [Create Anycast Gateways, on page 487](#). Choose **Extended Node** as the **Pool Type**.
- Cisco DNA Center configures the extended IP address pool and VLAN on the supported fabric edge device. This enables the onboarding of extended nodes.
- Step 3** Configure the DHCP server with the extended IP address pool and Option 43. Ensure that the extended IP address pool is reachable from Cisco DNA Center.
- Note** For a detailed description of Option 43, see [DHCP Controller Discovery, on page 369](#).
- Step 4** Connect the extended node device to the fabric edge device. You can have multiple links from the extended node device to the fabric edge.
- Step 5** Create a port channel on the fabric edge node that is connected to the extended node. For a subsequent extended node in a ring or daisy chain, create the port channel on the previous extended node it connects to.
- Note** Complete this step only if the global authentication mode for the fabric is **Open Authentication, Low Impact**, or **Closed Authentication**. If the fabric site is set to **None** authentication mode, the port channel is automatically created during the onboarding of the extended nodes using Plug and Play provisioning.

To create a port channel, complete the following steps:

- a) Click the menu icon () and choose **Provision > Fabric Sites**.
- b) In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.
- c) Select a fabric site.
- d) In the **Fabric Infrastructure** tab, choose a fabric edge node (or an extended node, depending on the connection).
- e) In the slide-in pane, under the **Port Channel** tab, click **Create Port Channel**.
- f) Complete the following:

- Choose an **Extended Node** in the **Connected Device Type** drop-down list.
- Enter a description.
- Choose **Port Aggregation Protocol (PAgP Desirable)**.
Starting with Cisco IOS XE Release 17.1.1s, IE 3300 and IE 3400 devices support PAgP.
- Select **On** for IE 3300 and IE 3400 devices if they are running versions earlier than Cisco IOS XE Release 17.1.1s.
Note Link Aggregation Control Protocol (LACP) doesn't work for extended node onboarding.
- Choose the ports to be bundled as a port channel.

g) Click **Done**.

This creates a port channel on the fabric edge node (or the extended node) to onboard an extended device.

Step 6 Power up the extended node device if it has no previous configuration. If the extended node device has configurations, reset the device configuration to factory default and reload it.

Cisco DNA Center adds the extended node device to the Inventory and assigns the same site as the fabric edge. The extended node device is then added to the fabric. Now the extended node device is onboarded and ready to be managed.

After the configuration is complete, the extended node appears in the fabric topology with a tag (X) to indicate that it is an extended node.

Upgrade an Extended Node to a Policy Extended Node

Cisco SD-Access automation onboards a policy extended node-capable device with a Cisco DNA Essentials license as an extended node. You can convert this extended node device to a policy-extended node by upgrading its license to Cisco DNA Advantage.

In a daisy chain, you cannot upgrade an extended node to a policy extended node if its upstream device is an extended node.

In a ring, you cannot upgrade an extended node to a policy extended node if both its neighbors are extended nodes.

After you upgrade the node to policy extended node, you cannot reconfigure it as an extended node.

To convert an extended node to a policy extended node, do the following.

Before you begin

- Ensure that the extended node is already onboarded.
- Update the Smart Licensing credentials on Cisco DNA Center.

Step 1 Change the license level on the device from Cisco DNA Essentials to Cisco DNA Advantage, using the Cisco DNA Center License Manager:

- a) Click the menu icon (☰) and choose **Tools > License Manager**.

- b) In the **Devices** tab, select the device.
- c) Choose **Actions > Change License > Change DNA License**.
- d) In the **Change DNA License Level** window, click **Advantage**.
- e) Click **Confirm**.
- f) In the **Success** message window, click **OK**.

The device reloads.

Step 2 Wait for the node to become **Reachable** and get to the **Managed** state.

The **Provision > Network Devices > Inventory** window displays the reachability status of all the devices.

Step 3 If you see a **Netconf Connection Refused** error, resynchronize the device. Repeat the resynchronization process until the error is no longer displayed.

- a) In the **Provision > Network Devices > Inventory** window, select the device.
- b) Choose **Actions > Inventory > Resync Device**.

Step 4 Upgrade to policy extended node.

- a) In the **Provision > Fabric Sites** window, select the site in which the device is onboarded.
- b) In the **Fabric Infrastructure** tab, click a device to edit its attributes.
- c) In the **Fabric** tab, click the **Policy** toggle button under **Extended Node Attributes**.
- d) In the **Policy Extended Node Upgrade** window that is displayed, click **Upgrade**.

Delete an Extended Node

This task describes the steps to delete an extended node, policy extended node, and authenticated extended node.

Step 1 Remove the extended node device from the fabric.

- a) Click the menu icon (**☰**) and choose **Provision > Fabric Sites**.
- b) In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.
- c) Select the fabric site that contains the extended node device.
- d) In the **Fabric Infrastructure** tab, click the extended node device.
- e) In the slide-in pane, click **Remove From Fabric**.
- f) Click **Add**.

Step 2 Delete the device from **Inventory**.

For steps to delete the device from inventory, see [Delete a Network Device, on page 102](#).

Step 3 For a supplicant-based extended node device, delete the port assignment configuration in the fabric edge node or the FIAB.

Configure a REP Ring Topology for Extended Nodes and Policy Extended Nodes

To enable redundancy with a recovery time of less than 50 ms for network failures with extended nodes, configure a Resilient Ethernet Protocol (REP) ring for the fabric site.

Unless explicitly stated, the term *extended node* also represents a policy extended node.

The following devices can be configured in a REP ring:

- Extended Node:

Cisco Industrial Ethernet (IE) 4000, 4010, 5000 series switches that operate Cisco IOS 15.2(7)E3 and later releases.

Cisco Catalyst IE3300 series switches that operate Cisco IOS XE 17.3.3 and later releases.

- Policy Extended Node:

Cisco Catalyst IE3400, IE3400H series switches that operate Cisco IOS XE 17.3.3 and later releases.

Limitations of a REP Ring

- To add an extended node into an existing REP ring, first delete the REP ring. Deleting the REP ring enables the Per VLAN Spanning Tree Protocol (PVSTP), which avoids Layer 2 loops. Then, add the new extended node to the fabric and recreate the REP ring to include the new extended node.
- Multiple rings within a given REP ring and a ring of rings aren't supported.
- A node in a REP ring can have other nodes connected to it in a daisy chain manner. However, a node in a daisy chain can't have a ring of nodes connected to it.
- A REP ring or a daisy chain can't be a mix of extended nodes and policy extended nodes. A REP ring or a daisy chain must consist entirely of either extended nodes or policy extended nodes.
- By default, a maximum of 18 devices can be onboarded in a single REP ring. To onboard more than 18 devices, increase the BPDU timer using **spanning-tree vlan *infra VN VLAN* max-age 40** command. Use the Cisco DNA Center templates to configure the command.

Note that in some rare instances, when the last two nodes of the ring try to onboard simultaneously, a port channel might not be created between these nodes. A port channel is established between the last two nodes of the ring when a REP ring is created.

Unless otherwise stated, the following steps are applicable to both extended node and policy extended node.

Before you begin

Ensure that you have onboarded the fabric edge nodes and extended nodes.

Identify the fabric edge node and its interfaces that terminate the REP ring.



Note The REP ring configuration procedure may disrupt the network traffic for a brief period.

Step 1 Click the menu icon (☰) and choose **Workflows > Configure REP Ring**.

Alternatively, you can navigate to the Fabric Site topology view, select the Fabric Edge node or the FIAB node on which you want to create the REP ring and click **Create REP Ring** under the **REP Rings** tab.

- Step 2** If a task overview window appears, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Select a fabric site** window, select a site that has both edge node and extended nodes.
- Step 4** In the **Select a fabric edge node** window, choose a fabric edge node.
- Step 5** In the **Select Extended Nodes connected to Fabric Edge** window, choose the extended nodes that connect to the fabric edge node.

You can choose two extended nodes to connect to the fabric edge node.

- Step 6** Review and edit (if necessary) your fabric site, edge node, and extended node selections.

- Step 7** To initiate the REP ring configuration, click **Provision**.

You can see a detailed status of the configuration progress on the **REP Ring Configuration Status** window.

- Step 8** The **REP Ring Summary** window displays the details of the REP ring that is created along with the discovered devices.
- Step 9** After the creation of the REP ring, a success message is displayed.

To verify the creation of the REP ring, go to the fabric site window and click the fabric edge node.

In the slide-in window, under the **REP Ring** tab, you can see the list of all REP rings that exist on that edge node.

Click a REP ring name in the list to view its details, such as the devices present in the ring, ports of each device that connect to the ring, and so on.

View REP Ring Status

To view the status of the devices in an REP ring, do the following:

-
- Step 1** In the Cisco DNA Center GUI, click the menu icon (☰) and choose **Provision > Fabric Sites**.

- Step 2** In the **Fabric Sites** tab, click the number that indicates the count of fabric sites.

- Step 3** Select a fabric site from the list that displays all the fabric sites.

- Step 4** In the **Fabric Infrastructure** tab, click the fabric edge node or the fabric in a box (FIAB).

A slide-in pane displays the details of the fabric edge node or the FIAB that is selected.

- Step 5** In the **REP Rings** tab, click **View** to see the **REP Ring Topology Status**.

The **REP Topology Status** section displays the current state of all the devices in the REP ring. The state, as displayed in the **Role** column, can be **Open**, **Fail**, or **Alt**.

Open indicates that the device link is up and that it is forwarding traffic.

Fail indicates that the device link is down.

Alt indicates that the device link is up, but the port cannot forward traffic.

Delete a REP Ring

- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** In the **Fabric Infrastructure** tab, click the fabric edge node that terminates the REP Ring.
A slide-in window displays the details of the fabric edge node selected.
- Step 3** In the **REP Rings** tab, for the desired REP Ring, click **Actions (...)** > **Delete**.
This deletes the REP Ring.
-

Delete a Node from a REP Ring

This task describes the steps to delete one extended node or multiple extended nodes from a REP ring.



Note After the extended nodes are removed, the downsized REP ring should use the existing interfaces to create a link to the neighboring devices.

Before you begin

Ensure that the REP ring to which the node belongs is not incomplete.

- Step 1** Manually remove the extended node devices from the network.
Alternatively, if a device in a REP ring goes down, the **Fabric Infrastructure** window displays a notification.
- Step 2** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 3** In the **Fabric Infrastructure** tab, click the fabric edge node that terminates the REP ring.
A slide-in pane displays the details of the selected fabric edge node.
- Step 4** In the **REP Rings** tab, for the desired REP ring, choose **Actions (...)** > **Rediscover**.
The extended node device is deleted from the REP ring and the REP ring display is updated.
-

Configure Supplicant-Based Extended Nodes

Supplicant-based extended nodes, also called Authenticated Extended Nodes (AENs), are extended node devices that receive an IEEE 802.1x (Dot1x) supplicant configuration and are onboarded into the SD-Access network only after a complete authentication and authorization. To onboard a supplicant-based extended node device, the authenticator port on the fabric edge must be configured with a Closed Authentication Template.

The following platforms support supplicant-based extended node onboarding:

Fabric Edge or FIAB:

Cisco Catalyst 9000 Series – C9300, C9400, C9500, and C9500H switches that operate Cisco IOS XE 17.7.1 or later.



Supplicant-based Extended Node:

Cisco Catalyst 9000 Series – C9200, C9300, C9400, C9500, and C9500H switches that operate Cisco IOS XE 17.7.1 or later.

Steps to Configure a Supplicant-Based Extended Node

Before you begin

- Configure Cisco ISE and ensure that it operates Release 3.1 or later. See [Configure Cisco Identity Services Engine to Onboard Supplicant-Based Extended Node](#), on page 505.
- Add the fabric edge node or FIAB device to the fabric and ensure that it operates Cisco IOS XE 17.7.1 or later.
- Set the Path MTU appropriately for the path between the fabric edge node and Cisco ISE. We recommend a value of 9100. Note that the Path MTU is set for all the devices in the fabric during LAN automation or when the underlay is configured.

-
- Step 1** Configure AAA server settings in Cisco DNA Center.
- a) Define Cisco ISE as the AAA server for device authentication in the **System > Settings > External Services > Authentication and Policy Servers** window.
For the complete procedure, see "Configure Authentication and Policy Servers" in the [Cisco DNA Center Administrator Guide](#).
 - b) Add the Cisco ISE server to the global site. For information, see [Add Cisco ISE or Other AAA Servers](#), on page 192.
- Step 2** (Optional) Configure Cisco DNA Center to authorize the device before onboarding.
- a) Click the menu icon () and choose **System > Settings > Device Settings > PnP Device Authorization**.
 - b) Check the **Device Authorization** check box to enable authorization on the device.
 - c) Click **Save**.
- Step 3** Configure the Cisco DNA Center appliance to manage your PKI certificates.
- a) Click the menu icon () and choose **System > Settings > Trust & Privacy > PKI Certificates**.
 - b) In the **PKI Certificates** window, click **Use Cisco DNA Center**.
 - c) In the **CA Management** tab, click **Download CA Certificate**.
 - d) Add the certificate to the Cisco ISE Trusted Certificate Store. For more information, see the [Cisco Identity Services Engine Administrator Guide](#).
- If you use an external certificate, add that certificate to the Cisco ISE Trusted Certificate Store.
- Step 4** Configure the DHCP server with the extended IP address pool and Option 43. Ensure that the extended IP address pool is reachable from Cisco DNA Center.
For a detailed description of Option 43, see [DHCP Controller Discovery](#), on page 369.
- Step 5** Enable **Closed Authentication** and disable Bridge Protocol Data Unit (BPDU) Guard on the fabric Site.

By default, selecting Closed Authentication pushes the BPDU Guard configuration on all the downlink access ports. When a remote switch like an extended node is connected, BPDU Guard pushes the port to error disabled mode. To disable BPDU Guard, uncheck the **Enable BPDU Guard** check box during the Closed Authentication configuration.

For more information, see [Select an Authentication Template](#).

Step 6 Assign an extended IP address pool to INFRA_VN, as described in [Create Anycast Gateways, on page 487](#).

In the **Create Anycast Gateways** workflow, choose **Extended Node** as the **Pool Type** and check the **Supplicant-Based Extended Node Onboarding** check box.

Cisco DNA Center configures the extended IP address pool and VLAN on the supported fabric edge device. This enables the onboarding of extended nodes.

Note Extended IP address pool is successfully assigned only if the fabric edge devices operate Cisco IOS XE 17.7.1 or later. If you upgraded from an earlier release of Cisco DNA Center, the supplicant-based extended node migration must be complete before configuring the extended IP address pool.

Step 7 Connect the extended node device to the fabric edge node or the FIAB.

After powering on, the extended node device is in **Pending Authorization** state if you chose to authorize the device before onboarding (Step 2). You can check the status of the device in the **Provision > Plug and Play** window.

Step 8 (Optional) Authorize the device.

Perform this step only if the device is in **Pending Authorization** state.

- a) Click the menu icon (☰) and choose **Provision > Plug and Play**.
- b) In the **Plug and Play** window, select the supplicant-based extended node device and choose **Actions > Authorize**.

The authorization process provisions the supplicant-based extended node device for completing a certificate-based EAP-TLS authentication with Cisco ISE. After authentication, Cisco ISE authorizes the supplicant-based extended node device for complete access. The supplicant-based extended node device is then fully onboarded into the SD-Access fabric.

After a supplicant-based extended node device is onboarded into the fabric, access to the fabric edge-supplicant port is only based on authentication status. If the device or the port goes down, the authentication session is cleared, and traffic is not allowed on the port. When the port comes up again, it goes through the IEEE 802.1X (Dot1x) authentication process to regain access to the SD-Access network.

Replace a Faulty Port

If the link between the authenticator (fabric edge or FIAB) port and the supplicant port goes down, you can replace the faulty port and configure a new port through the **Port Assignment** menu.

Step 1 To replace the supplicant port, follow these steps:

- a) Clear the configuration on the new supplicant port.
- b) Copy the existing configuration from the current supplicant port to the new supplicant port to allow 802.1X authentication.

Step 2 To replace the authenticator port, follow these steps:

- a) Assign the supplicant port to the new interface of the authenticator. For information on port assignment, see [Configure Ports Within the Fabric Site, on page 482](#). Choose **Supplicant-Based Extended Node** as the **Connected Device Type**.
- b) Clear the existing port assignment on the old interface of the authenticator.

Step 3 Disconnect the physical connection between the old ports of the authenticator and the supplicant. Connect a cable between the new ports of the authenticator and the supplicant. Bring this link up.

Step 4 After the link between the new ports of the authenticator and supplicant is up, follow these steps:

- a) Resynchronize the device information in Cisco DNA Center by performing an **Inventory > Resync Device** for both the authenticator and the supplicant. See [Resynchronize Device Information, on page 102](#).
- b) Assign the new supplicant port to the authenticator. For information on port assignment, see [Configure Ports Within the Fabric Site, on page 482](#). Choose **Authenticator Switch** as the **Connected Device Type**.
- c) Clear the port assignment on the old supplicant port.

Configure Cisco Identity Services Engine to Onboard Supplicant-Based Extended Node

This task describes how to profile an Supplicant-Based Extended Node (SBEN) device in Cisco Identity Services Engine (ISE). The steps listed below are part of the Cisco ISE configuration procedure. For more information, refer the [Cisco Identity Services Engine Administrator Guide](#).

Before you begin

Download the CA certificate from Cisco DNA Center.

Step 1 Import the CA certificate into Cisco ISE:

From the Cisco ISE home page, choose **Administration > System > Certificates > System Certificates > Import**. In the **Import** window, ensure that you select the **Trust for client authentication and Syslog** check box. For more information, see the "Import the Root Certificates to the Trusted Certificate Store" section in the [Cisco Identity Services Engine Administrator Guide](#).

Step 2 Configure the following authorization profiles with their RADIUS attributes:

From the Cisco ISE main menu, choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

Configure the following profiles:

SBEN-DHCP :

```
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_DHCP_ACL.in
```

SBEN_LIMITED_ACCESS_AUTHZ :

```
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_MAB_ACL.in
cisco-av-pair = interface-template-name=SWITCH_SBEN_MAB_TEMPLATE
```

SBEN_FULL_ACCESS_AUTHZ :

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=SWITCH_SBEN_FULL_ACCESS_TEMPLATE
```

Step 3 Define the device profiling policy in the **Profiling Policies** window.

- a) From the Cisco ISE main menu, choose **Policy > Profiling > Profiling Policies**.
- b) In the **Profiling Policies** window, add a new **DHCP-v-i-vendor-class** condition for the **Cisco-Device: Cisco-Switch** policy.

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

Create an Identity Group for the policy Yes, create matching Identity Group
 No, use existing Identity Group hierarchy

Parent Policy

* Associated CoA Type

System Type



Rules

If	Condition	Then	Value
If	Condition <input type="text" value="Cisco-IO-NMAPOSCheck"/>	Then <input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>
If	Condition <input type="text" value="CDP_cdpCachePlatform_CONTAINS_9200..."/>	Then <input type="text" value="Certainty Factor Increases"/>	<input type="text" value="20"/>
If	Condition <input type="text" value="DHCP_v-i-vendor-class_CONTAINS_9200..."/>	Then <input type="text" value="Certainty Factor Increases"/>	<input type="text" value="20"/>

Condition Name	Expression	Operator	Value
<input type="text" value="DHCP:v-i-ven..."/>	<input type="text" value="CONTAIN"/>	<input type="text" value="9200"/>	OR
<input type="text" value="DHCP:v-i-ven..."/>	<input type="text" value="CONTAIN"/>	<input type="text" value="9300"/>	
<input type="text" value="DHCP:v-i-ven..."/>	<input type="text" value="CONTAIN"/>	<input type="text" value="9500"/>	

- c) Create a new child policy for the supplicant device, under **Cisco-Switch** and apply the **CdpCachePlatform** and **V-I-Vendor-Class** conditions.

Ensure that the **Minimum Certainty Factor** value for the child policy is higher than that of the parent policy.

* Name	CAT9K_EN	Description	<input type="text"/>
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	30	(Valid Range 1 to 65535)	
* Exception Action	NONE	▼	
* Network Scan (NMAP) Action	NONE	▼	
Create an Identity Group for the policy	<input checked="" type="radio"/> Yes, create matching Identity Group <input type="radio"/> No, use existing Identity Group hierarchy		
* Parent Policy	Cisco-Switch	▼	
* Associated CoA Type	Global Settings	▼	
System Type	Administrator Created		
Rules			
If Condition	CDP_odpCachePlatform_CONTAINS_C92...	▼	Then Certainty Factor Increases ▼ 30 
If Condition	DHCP_v-i-vendor-class_CONTAINS_C920...	▼	Then Certainty Factor Increases ▼ 30 

Step 4 Set the global Change of Authorization (CoA) type to **Reauth**.

To configure the **CoA Type**, from the Cisco ISE home page, navigate to **Work Centers > Profiler > Settings**.

Choose **Reauth** from the **CoA Type** drop-down list.

Step 5 Define the authorization policy in the **Authorization Policy** window.

- From the Cisco ISE home page, choose **Policy > Policy Sets > Default > Authorization Policy**.
- Ensure that the default MAB policy is set to **CONTINUE** option for the **If User not found** field.

- In the **Authorization Policy** window, configure the authorization policies for the supplicant device and associate the policies with the authorization profiles that were created earlier (SBEN-DHCP, SBEN_LIMITED_ACCESS_AUTHZ, SBEN_FULL_ACCESS_AUTHZ).

Configure a Port Channel

A group of ports bundled together to act as a single entity is called a port channel. Port channels between a fabric edge and its remotely connected devices, such as extended nodes or servers, increase the connection resiliency and bandwidth.

Create a Port Channel

Before you begin

The authentication must be **Closed Authentication**.




Note The following steps are automated for other authentication modes.

- Step 1** Click the menu icon (☰) and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** Select a fabric site.
- Step 4** In the **Fabric Infrastructure** tab, click a fabric edge node.
- Step 5** In the **Port Channel** tab of the slide-in pane, click **Create Port Channel**.
- Step 6** From the **Connected Device Type** drop-down list, choose the type of connected device:
- To create a port channel between a fabric edge node and an extended node or between two extended nodes, choose **Extended Node**.
 - To create a port channel with a fabric edge node or extended node on one side and a third-party device or a server port on the other side, choose **Trunk**.
- Step 7** Enter a **Description** for the new port channel.
- Step 8** Choose a protocol:
- For the extended nodes that run Cisco IOS XE Release 16.12.1s and earlier releases, choose **On** as the protocol.
 - For the extended nodes that run Cisco IOS XE Release 17.1.1s and later releases, choose **Port Aggregation Protocol (PAgP)** as the protocol.
 - Don't select **Link Aggregation Control Protocol (LACP)** as the protocol for extended nodes. You can only connect the trunk ports or the server ports in the LACP mode.
- Step 9** From the list of ports displayed, choose the ports to be bundled.
- Note** You cannot have more than 16 members in a port channel that is connected in the LACP mode.
You cannot have more than eight members in a port channel that is connected in the PAgP mode.
- Step 10** Click **Done**.
-


Update a Port Channel

Before you begin

Ensure that at least one member interface exists before you update a port channel.

- Step 1** Click the menu icon () and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** Select a fabric site.
- Step 4** In the **Fabric Infrastructure** tab, click a fabric edge node.
- Step 5** In the slide-in pane, click the **Port Channel** tab.
- Step 6** From the list of port channels displayed, click the port channel to be updated.
- The resulting window displays all the interfaces and the status of the selected port channel.
- Step 7** Update the port channel.
- You can either add interfaces to the port channel or delete existing interfaces on the port channel.
- Step 8** Click **Done**.
-

Delete a Port Channel

- Step 1** Click the menu icon () and choose **Provision > Fabric Sites**.
- Step 2** Under **SUMMARY**, click the number that indicates the count of fabric sites.
- Step 3** Select a fabric site.
- Step 4** In the **Fabric Infrastructure** tab, click a fabric edge node.
- Step 5** In the slide-in pane, click the **Port Channel** tab.
- The **Port Channel** view lists all the existing port channels.
- Step 6** Check the check box for the port channel and click **Delete**.
- Step 7** At the prompt, click **Yes**.
-

Multicast

Multicast traffic is forwarded in different ways:

- Through shared trees by using a rendezvous point. PIM SM is used in this case.
- Through shortest path trees (SPT). PIM source-specific multicast (SSM) uses only SPT. PIM SM switches to SPT after the source is known on the edge router that the receiver is connected to.

See [IP Multicast Technology Overview](#).

Configure Multicast

Cisco DNA Center provides a workflow to enable group communication or multicast traffic in virtual networks. The workflow also allows you to choose multicast implementation in the network: native multicast or headend replication.



Note You can enable multicast on a virtual network whose border serves as a multisite remote border. Configuring multicast on such a virtual network configures multicast on the devices in the inherited virtual network too, provided the inherited virtual network already contains a segment. If the inherited virtual network doesn't have a segment, multicast is deployed only after the first segment is created. Ensure that a virtual network and its inherited networks deploy the same type of multicast implementation. The edge node devices of an inherited virtual network cannot be configured as a rendezvous point (RP).

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure Multicast**.
- Step 2** If a task overview window appears, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Fabric Site** window, select a site in the site hierarchy pane.
- Step 4** In the **Replication Mode** window, choose the method of multicast implementation for the network from the following:
- **Native Multicast**
 - **Head-end replication**
- Step 5** In the **Virtual Networks** window, select the virtual network for which you want to set up multicast.
- Note** You can't select an inherited virtual network to set up multicast.
- Step 6** In the **Multicast pool mapping** window, select an IP address pool from the **IP Pools** drop-down list. The selected IP address pool is associated with the chosen virtual network.
- Step 7** In the **Multicast Mode** window, choose the type of multicast to implement:
- **SSM** (Source Specific Multicast)
 - **ASM** (Any Specific Multicast)
 - Select **SSM** and **ASM** to configure both together.
- Step 8** Do the following:
- a) On selecting **SSM**, configure the SSM list by adding an IP group range for each virtual network. You can add multiple IP group ranges for a virtual network.
 1. By default, 232.0.0.0/8 range of IPv4 address is selected. You can optionally modify the IPv4 address range.
Choose an IP group range from 225.0.0.0 to 239.255.255.255.
 2. For IPv6 addresses, FF3x::/32 is reserved for SSM.

- b) On selecting **ASM**, in the **Multicast Group to Rendezvous Point Mapping** window, configure the rendezvous point for each virtual network:
1. Choose the type of rendezvous point: **External** or **Fabric**.
 2. Configure the rendezvous points in the respective tabs: **IPv4 RP** and **IPv6 RP**.
 3. You can define any number of external rendezvous points.
 4. Optionally, you can define a group-to-rendezvous point mapping. There could be one or multiple IPv4/IPv6 multicast groups that are associated with a rendezvous point.
 5. You can either have a rendezvous point with no mapping or with mapping. Both can't be configured together.
 6. The permitted multicast group ranges for IPv6 and IPv4 FF00:/8 and 225.0.0.0/8 - 239.0.0.0/8 respectively.

Step 9 In the **Summary** window, review the multicast settings. To modify any of the settings, click **Edit**.

Step 10 In the **Deploy Multicast** window, click **Now** or **Later** to indicate when you want to start the multicast configuration. Click **Deploy** to complete the configuration.



CHAPTER 22

Provision Services

- [Applications, on page 513](#)
- [Application Hosting, on page 529](#)
- [Application Hosting on Cisco Catalyst 9100 Series Access Points, on page 537](#)
- [Configure a Site-to-Site VPN, on page 539](#)
- [Create a User-Defined Network Service, on page 541](#)
- [Configure Cisco Umbrella, on page 543](#)
- [Create Secure Tunnel, on page 550](#)

Applications

The following sections provide information about applications.

About Application Visibility

The Application Visibility service lets you manage your built-in and custom applications and application sets.

The Application Visibility service, hosted as an application stack within Cisco DNA Center, lets you enable the Controller-Based Application Recognition (CBAR) function on a specific device to classify thousands of network and home-grown applications and network traffic.

You can install the following packages:

- **Application Policy:** Lets you automate QOS policies across LAN, WAN, and wireless within your campus and branch.
- **Application Registry:** Lets you view, manage, and create applications and application sets.
- **Application Visibility Service:** Provides application classification using Network-Based Application Recognition (NBAR) and CBAR techniques.

NBAR supports provisioning of up to 450 interfaces on Cisco Catalyst 9000 devices. Cisco DNA Center Application Visibility does not exceed this 450-interface limit.

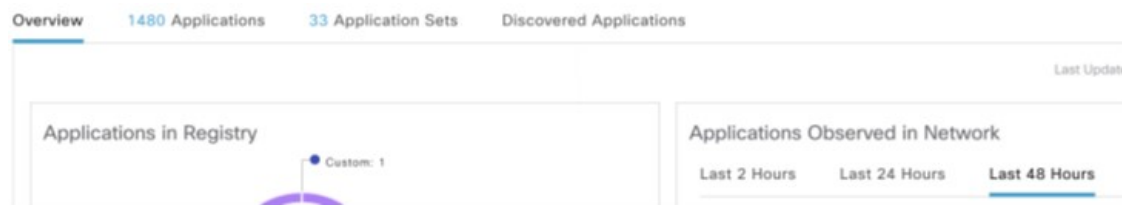


Note To ensure compatibility, the preceding packages must have the same package version.

If you install Application Registry or both Application Registry and Application Policy, you can see the **Applications** and **Application Sets** tabs when you click the menu icon (☰) and choose **Provision > Services > Application Visibility**.



If you install Application Registry and Application Visibility Service or Application Registry, Application Policy, and Application Visibility Service, you can see the **Applications**, **Application Sets**, and **Discovered Applications** tabs when you click the menu icon (☰) and choose **Provision > Services > Application Visibility**.



The Application Visibility service has the following phases:

- Day 0: First-time service enablement.
- Day N: Ongoing monitoring and configuration changes.

Day 0 Setup Wizard to Enable the Application Visibility Service

Follow the Day 0 **Setup** wizard to enable the Application Visibility service in Cisco DNA Center.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
You can view a brief introduction about the Application Visibility feature.
- Step 2** In the **Application Visibility** window, click **Next**.
A dialog box for enabling the Application Visibility service is displayed.
- Step 3** Click **Yes** to enable CBAR on Cisco DNA Center.
- Step 4** Check the **Enable CBAR on all Ready Devices** check box or choose devices with **CBAR Readiness Status** in **Ready** state.

If you want to choose a device that is not ready for enabling CBAR, follow the info message to move it to Ready state before proceeding in the **Setup** wizard.
- Step 5** Click **Next** to enable CBAR on the devices.
- Step 6** Choose an external authoritative source, such as Microsoft Office 365 Cloud Connector, to either help classify the unclassified traffic or help generate improved signatures.
- Step 7** If you want to exclude interfaces in the Application Visibility service, do the following:
- a) In the **Enable CBAR** slide-in pane, search for the device name or locate the device and click **View Interfaces**.

- b) Locate the interface that you want to exclude.
- c) In the **Status** column, click the toggle button to disable the interface.

By default, **All** is enabled in the **Show** toggle button, that displays all the available interfaces. You can choose **Excluded Interfaces** to view the excluded interfaces.

- d) Click **Save**.

Step 8 Click **Finish**.

The **Overview** window shows the application registry; device recognition method; device CBAR readiness; application observed in the network for the past 2, 24, or 48 hours (valid only if CBAR is enabled on at least one device); service health; and CBAR health score.

Day-N Application Visibility View

The Day-N Application Visibility page shows the application registry, device recognition method, device CBAR readiness, application observed in the network for the past 2, 24, or 48 hours (valid only in case CBAR was enabled on at least one device), and CBAR health.

The following table describes the charts that are available in the **Overview** tab in **Provision > Services > Application Visibility**.

Table 36: Day-N Application Visibility View: Charts

Chart	Description
Applications in Registry	<p>This chart displays the number of applications available in the Cisco DNA Center application registry that can be used in Application Policy. The applications are classified as follows:</p> <ul style="list-style-type: none"> • Custom: Applications added by a user • Built-in: Preinstalled applications in Cisco DNA Center • Discovered: Applications discovered by different recognition methods and imported into the application registry
Applications Observed in Network	<p>This chart shows the applications observed in the past 2, 24, or 48 hours and lists the applications with highest network traffic ratio.</p> <p>Note The chart shows the applications observed only on CBAR-enabled devices.</p>

Chart	Description
Devices by Active Recognition Method	<p>This chart displays the number of devices classified by each of the application recognition methods:</p> <ul style="list-style-type: none"> • CBAR-enabled devices: Routers and switches • NBAR-based devices: Routers, switches, Cisco Wireless Controllers, and Cisco Catalyst 9800 Series Wireless Controller • IP/port-based devices: Switches • Not supported devices: Devices that are not supported by any of the preceding methods
CBAR Readiness Status	<p>This chart displays the device count in each CBAR readiness status.</p> <ul style="list-style-type: none"> • Enabled: Devices that are CBAR-enabled • Ready: Devices that are ready for enabling CBAR <p>Note The info icon next to Ready status shows the respective device is wireless enabled.</p> <ul style="list-style-type: none"> • Not Ready: Devices that support CBAR but are not ready for enabling CBAR due to some issues • Not Supported: Devices that do not support CBAR
Service Health and CBAR Health	<p>This widget displays the service health and the average health score for all CBAR-enabled devices. The device is healthy if there are no outstanding errors or warnings on that device.</p> <p>The CBAR health score is calculated across all CBAR-enabled devices.</p> <p>You can view the CBAR health of each CBAR-enabled device. A 0% CBAR health score indicates that the device has at least one error (P1). A 50% CBAR health score indicates that the device has no errors but has at least one warning (P2). A 100% CBAR health score indicates a healthy device.</p> <p>This widget also shows the service issues and remedies (P1, P2, and P3). The green tick mark indicates healthy service. The red cross mark indicates at least one P1 issue. The warning icon indicates at least one P2 issue. Click P1, P2, and P3 to view more about the services issues and remedies.</p>
CBAR Health Issues and Remedies	<p>All issues are classified by priority:</p> <ul style="list-style-type: none"> • Errors (P1) • Warnings (P2) • Others (P3) <p>Click the P1, P2, and P3 tabs to view the device issues and remedy details.</p>

Site Devices Table: This table provides device information and statuses. You can filter the devices using the **Quick Filter** and **Device Table Filter**.

Table 37: Day-N Application Visibility View: Site Devices Table

Column	Description
Device Name	Name of the device. Click the device name to view the CBAR Service Status.
Management IP	IP address of the device.
Device Type	Group of related devices, such as routers, switches and hubs, or wireless controllers.
Site	The site to which the device is assigned.
Fabric	The fabric domain to which the device is assigned.
Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Cisco DNA Center cannot determine a device role, it sets the device role to Unknown.
Active Recognition Method	Shows the device recognition method (CBAR, NBAR, IP/Port, or Not Supported).
OS Version	Cisco IOS software that is currently running on the device.
CBAR Readiness Status	Hover over the status displayed in the CBAR Readiness Status column to view the Remedy message.
Protocol Pack Version	Shows the current version of the protocol pack installed on the device and the protocol pack update status.
Device Registry Status	Shows the synchronization status of the device with the application registry. Hover over the info icon or the error icon to view more details about the synchronization status.
Deployment Status	Shows the CBAR deployment status. For more information, see Reconfigure CBAR, on page 518 .
Service Health Status	Click the issues in the Service Health Status column to open the CBAR Service status page, which displays a complete list of issues and the service status information of a device. If you click the Cisco Catalyst 9K device name, you can view the footprint (service load, CPU, and flows) of the CBAR service.
Application QoS Policy	The application policy applied to the device. For Cisco Wireless Controllers with more than one application policy, the number of application policies applied and the name of all the applied application policies are displayed.
WAN Interfaces	Shows the number of WAN interfaces. Click the WAN interface details to view the WAN connectivity settings for the device.

Reconfigure CBAR

You can include or exclude interfaces from **Site Devices** table in the **Overview** window.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
- Step 2** In the **Overview** page, scroll down to view the **Site Devices** table.
- Step 3** Click **Re-Configure** in the **Deployment status** column for the device you want to configure and do the following:
- In the **Enable CBAR** slide-in pane, search for the device name or locate the device and click **View Interfaces**.
 - Locate the interface that you want to exclude.
 - In the **Status** column, click the toggle button to disable the interface and click **Save**.
- Step 4** To include interfaces, choose **Excluded Interfaces** and enable the toggle button next to the desired interfaces, and click **Save**.
- Step 5** Click **Enable**.
-

What to do next

Applications and Application Sets

Applications are the software programs or network signaling protocols that are used in your network. Cisco DNA Center supports all of the applications in the Cisco Next Generation Network-Based Application Recognition (NBAR2) library of approximately 1400 distinct applications.

Applications are grouped into logical groups called application sets. An application set can be assigned a business relevance within a policy.

Applications are mapped into industry standard-based traffic classes, as defined in RFC 4594, that have similar traffic treatment requirements. The traffic classes define the treatments (such as Differentiated Services Code Point [DSCP] marking, queuing, and dropping) that will be applied to the application traffic, based on the business relevance group that is assigned.

If you have additional applications that are not included in Cisco DNA Center, you can add them as custom applications and assign them to application sets.

Unidirectional and Bidirectional Application Traffic

Some applications are completely symmetrical and require identical bandwidth provisioning on both ends of the connection. Traffic for such applications is described as bidirectional. For example, if 100 kbps of Low-Latency Queueing (LLQ) is assigned to voice traffic in one direction, 100 kbps of LLQ must also be provisioned for voice traffic in the opposite direction. This scenario assumes that the same Voice over IP (VoIP) coder-decoders (codecs) are being used in both directions and do not account for multicast Music-on-Hold (MoH) provisioning. However, certain applications, such as streaming video and multicast MoH, are most often unidirectional. Therefore, it might be unnecessary, and even inefficient, to provision any bandwidth guarantees for such traffic on a branch router for the branch-to-campus direction of traffic flow.

Cisco DNA Center lets you specify whether an application is unidirectional or bidirectional for a particular policy.

On switches and wireless controllers, NBAR2 and custom applications are unidirectional by default. However, on routers, NBAR2 applications are bidirectional by default.

Custom Applications

Custom applications are applications that you add to Cisco DNA Center. An orange bar is displayed next to custom applications to distinguish them from the standard NBAR2 applications and application sets. For wired devices, you can define applications based on server name, IP address and port, or URL. You can define custom applications for Cisco Catalyst 9800 Series Wireless Controllers and not for Cisco AireOS controllers.

When you define an application according to its IP address and port, you can also define a DSCP value and port classification.

To simplify the configuration process, you can define an application based on another application that has similar traffic and service-level requirements. Cisco DNA Center copies the other application's traffic class settings to the application that you are defining.

Cisco DNA Center does not configure ACLs for port numbers 80, 443, 53, 5353, and 8080, even if they are defined as part of a custom application. If the custom application has a transport IP defined, Cisco DNA Center configures the application on the devices.



Note For a custom application to be programmed on devices when a policy is deployed, you must assign the custom application to one of the application sets defined in the policy.

Discovered Applications

Discovered applications are applications that are discovered by importing from recommended customization such as an Infoblox DNS server or by importing from the recommended unclassified applications flow.

The unclassified traffic can come from any flow that the CBAR-enabled device identifies but that is not recognized by the NBAR engine. In such cases, the applications that have a meaningful bit rate are reported as unclassified and can be imported and used as applications in Cisco DNA Center.

The Application Visibility service lets Cisco DNA Center connect with external authoritative sources like the Microsoft Office 365 Cloud Connector to help classify the unclassified traffic or help generate improved signatures.



Note You must configure an NBAR cloud connector before configuring the Microsoft Office 365 Cloud Connector.

The discovered applications are imported to the application registry.

Favorite Applications

Cisco DNA Center lets you flag applications that you want to configure on devices before all other applications. Flagging an application as a favorite helps to ensure that the QoS policies for your favorite applications get configured on devices. For more information, see [Processing Order for Devices with Limited Resources](#), on page 596.

When custom applications are created they are marked as favorite applications.

Although there is no limit to the number of applications that you can mark as favorites, designating only a small number of favorite applications (for example, fewer than 25) helps to ensure that these applications are treated correctly from a business-relevance perspective in deployments with network devices that have limited ternary content addressable memory (TCAM).

Favorite applications can belong to any business-relevance group or traffic class and are configured system-wide, not on a per-policy basis. For example, if you flag the Cisco Jabber video application as a favorite, the application is flagged as a favorite in all policies.

Keep in mind that not only can business-relevant applications be flagged as favorites, even business-irrelevant applications can be flagged as such. For example, if administrators notice a lot of unwanted Netflix traffic on the network, they might choose to flag Netflix as a favorite application (despite it being assigned as business-irrelevant). In this case, Netflix is programmed into the device policies before other business-irrelevant applications, ensuring that the business intent of controlling this application is realized.

Configure Applications and Application Sets


The following subsections describe the various tasks that you can perform in the context of applications and application sets.



Note You can edit or delete only custom and discovered applications. You can edit or delete a maximum of 100 custom and discovered applications at one instance. If you choose NBAR applications for editing or deleting, a notification message indicates the number of applications that can be edited or deleted, excluding the number of chosen NBAR applications.

Change an Application's Settings

You can change the application set or traffic class of an existing NBAR, custom, or discovered application.

- Step 1** Click the menu icon () and choose **Provision > Services > Application Visibility > Application**.
- Step 2** Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.
You can search applications based on their name, port number, and traffic class.
- Step 3** Click the application name.
- Step 4** In the dialog box, change one or both settings:
 - **Traffic Class:** Choose a traffic class from the drop-down list. Valid traffic classes are BROADCAST_VIDEO, BULK_DATA, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, NETWORK_CONTROL, OPS_ADMIN_MGMT, REAL_TIME_INTERACTIVE, SIGNALING, TRANSACTIONAL_DATA, VOIP_TELEPHONY.
 - **Application Set:** Choose an application set from the drop-down list. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 5 Click **Save**.

Create a Server Name-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

Step 1 Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.

Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

Step 4 In the dialog box, provide the necessary information in the following fields:

- **Application name:** Name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen are the only special characters allowed in the application name.
- **Type:** Method by which users access the application. Choose **Server Name** for applications that are accessible through a server.
- **Server name:** Name of the server that hosts the application.
- **Similar to:** Application with similar traffic-handling requirements. Click the radio button to select this option, and then select an application from the drop-down list. Cisco DNA Center copies the other application's traffic class to the application that you are defining.
- **Traffic class:** Traffic class to which the application belongs. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
- **Application set:** Application set is where you want the application to reside. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, custom applications, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.

Step 5 Click **OK**.


Create an IP Address and Port-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

Step 1 Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.


Step 2 Click the **Application** tab.

Step 3 Click **Add Application**.

- Step 4** In the **Application name** field, enter a name for the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. The underscore and hyphen are the only special characters allowed in the application name.
- Step 5** In the **Type** area, click the **Server IP/Port** radio button to indicate that the application is accessible through an IP address and port.
- Step 6** Check the **DSCP** check box and define a DSCP value. If you do not define a value, the default value is Best Effort. Best-effort service is essentially the default behavior of the network device without any QoS.
- Step 7** Check the **IP/Port Classifiers** check box to define the IP address and subnet, protocol, and port or port range for an application. Valid protocols are IP, TCP, UDP, and TCP/UDP. If you select the IP protocol, you do not define a port number or range. Click  to add more classifiers.
- Step 8** Define your application traffic-handling requirements using one of the following methods:
- **Similar To:** If your application has similar traffic-handling requirements as an existing application, click the **Similar To** radio-button and choose the application from the drop-down list. Cisco DNA Center copies the traffic class of the other application to the application that you are defining.
 - **Traffic Class:** If you know the traffic class that you want to define for your application, click the **Traffic Class** radio button and choose the traffic class from the drop-down list. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.
- Step 9** From the **Application Set** drop-down list, choose the application set to which the application will belong. Valid application sets are authentication-services, backup-and-storage, collaboration-apps, consumer-browsing, consumer-file-sharing, consumer-gaming, consumer-media, consumer-misc, consumer-social-networking, custom applications, database-apps, desktop-virtualization, email, enterprise-ipc, file-sharing, generic-browsing, generic-media, generic-misc, tunneling, local-services, naming-services, network-control, network-management, remote-access, saas-apps, signaling, software-development-tools, software-updates, streaming-media.
- Step 10** Click **OK**.

Create a URL-Based Custom Application

If you have applications that are not in Cisco DNA Center, you can add them as custom applications.

- Step 1** Click the menu icon () and choose **Provision > Services > Application Visibility**.
- Step 2** Click the **Application** tab.
- Step 3** Click **Add Application**.
The **Add Application** dialog box appears.
- Step 4** In the **Application name** field, enter the name of the custom application. The name can contain up to 24 alphanumeric characters, including underscores and hyphens. (Underscores and hyphens are the only special characters allowed in the application name.)
- Step 5** For **Type**, click the **URL** radio button.
- Step 6** In the **URL** field, enter the URL used to reach the application.
- Step 7** Configure the traffic class:
- To use the same traffic class as another application with similar traffic-handling requirements, click the **Similar To** radio button and choose an application from the drop-down list.

- To specify the traffic class, click the **Traffic Class** radio button and choose a traffic class from the drop-down list. Valid values are BULK_DATA, TRANSACTIONAL_DATA, OPS_ADMIN_MGMT, NETWORK_CONTROL, VOIP_TELEPHONY, MULTIMEDIA_CONFERENCING, MULTIMEDIA_STREAMING, BROADCAST_VIDEO, REAL_TIME_INTERACTIVE, and SIGNALING.

Step 8 From the **Application Set** drop-down list, choose an application set in which you want the application to reside.

Step 9 Click **OK**.

Edit or Delete a Custom Application

If required, you can change or delete a custom application.



Note You cannot delete a custom application that is directly referenced by an application policy. Application policies typically reference application sets and not individual applications. However, if a policy has special definitions for an application (such as a consumer or producer assignment or bidirectional bandwidth provisioning), the policy has a direct reference to the application. As such, you must remove the special definitions or remove the reference to the application entirely before you can delete the application.

Step 1 Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.

Step 2 Click the **Application** tab.


Step 3 Use the **Search**, **Show**, or **View By** fields to locate the application that you want to change.

You can search applications based on their name, port number, and traffic class.

Step 4 To edit the application:

- Click the application name and make the required changes. For information about the fields, see [Create a Server Name-Based Custom Application, on page 521](#), [Create an IP Address and Port-Based Custom Application, on page 521](#), or [Create a URL-Based Custom Application, on page 522](#).
- Click **OK**.

Note When policy is redeployed, the edited custom applications are not reconfigured on Cisco Catalyst 9800 Series Wireless Controller.

Step 5 To delete the application, click  in the application box, and then click **OK** to confirm.

Mark an Application as Favorite

You can mark an application as a favorite to designate that the application's QoS configuration must be deployed to devices before other applications' QoS configuration. An application marked as favorite has a yellow star next to it.

When you add or edit a policy, applications marked as a favorites are listed at the top of the application set.

Applications are configured system-wide, not on a per-policy basis. For more information, see [Favorite Applications, on page 519](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
 - Step 2** Click the **Application** tab.
 - Step 3** Locate the application that you want to mark as a favorite.
 - Step 4** Click the star icon.
-

Create a Custom Application Set

If none of the application sets fits your needs, you can create a custom application set.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
 - Step 2** Click the **Application Sets** tab.
 - Step 3** Click **Add Application Set**.
 - Step 4** In the dialog box, enter a name for the new application set.
Cisco DNA Center creates the new application set; however, it contains no applications.
 - Step 5** Click **OK**.
 - Step 6** Use the **Search**, **Show**, or **View By** fields to locate the application set.
You can search applications based on their name, port number, and traffic class.
 - Step 7** Locate the applications that you want to move into the new application set.
 - Step 8** Check the check box next to the applications that you want to move.
 - Step 9** Drag and drop the applications into the new application set.
-

Edit or Delete a Custom Application Set

If required, you can change or delete a custom application set.



Note You cannot delete a custom application set that is referenced by an application policy. You must remove the application set from the policy before you delete the application set.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
 - Step 2** Click the **Application Sets** tab.
 - Step 3** Use the **Search**, **Show**, or **View By** fields to locate the application set that you want to change.
You can search applications based on their name, port number, and traffic class.
 - Step 4** Do one of the following:
 - To edit the application set, drag and drop applications into or out of the application set. Click **OK** to confirm each change.


- To delete the application set, click  in the application set box, and then click **OK** to confirm.

Update the Protocol Pack on a CBAR-Enabled Device

You can upgrade the protocol pack on any device that supports CBAR to the latest or any specific protocol pack.

Before you begin

- Configure Cisco credentials on **System Settings**. For more information about configuring Cisco credentials, see the [Cisco DNA Center Administrator Guide](#).
- Devices must support CBAR.
- CBAR must be enabled on the device.
- Protocol packs for the device must be available on cisco.com.

Step 1 Click the menu icon () and choose **Provision > Services > Application Visibility**.

Step 2 In the Day-N **Overview** page, scroll down to view the **Site Devices** table.

Step 3 Check the status shown in the **Protocol Pack Version** column in the **Site Devices** table.

You can click the **Outdated** status to view the list of applicable protocols packs in the **Update Protocol Pack** window.

Step 4 Click **Update** corresponding to the required protocol pack version in the **Update Protocol Pack** window.

The **Protocol Pack Version** column shows **In progress** status. Click the info icon to view the current updating version. If the **Protocol Pack Version** column shows **Update failed** status, click the error icon to view the failure reason.

Step 5 If you want to update all the devices or selected devices to the latest protocol pack, do the following:

To update the protocol pack on all applicable CBAR-enabled devices:

- From the **Update Protocol Pack** drop-down list, choose **All Devices** and click **Yes** in the subsequent warning pop-up windows.

To update the protocol pack on the selected devices:

- Choose the devices in the **Site Devices** table.
- From the **Update Protocol Pack** drop-down list, choose **Selected Devices** and click **Yes** in the subsequent warning pop-up windows.

Discover Unclassified Applications

The Application Visibility service in Cisco DNA Center obtains information on classified and unclassified domains and sockets from devices and displays that information in the **Observed Traffic** chart. The number

of unclassified server names and IP/ports that are discovered by the Application Visibility service is shown under **Recommendations**.

You can add the unclassified server names and IP/ports to the Application Registry.



Note You can add a maximum of 1100 discovered applications in the Application Registry.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
- Step 2** Click the **Discovered Applications** tab.
- Step 3** Under **Recommendations**, click the **discovered server names** link or the **discovered IP/Ports** link.
The table lists the discovered servers or IP/ports that are not classified. Choose the server and check the **Hide Ignored Applications** check box if you want to hide the selected server or IP/ports in the table.
- Step 4** Choose the server or IP/ports that you want to import as an application in the Application Registry.
- Step 5** Choose the required **Application**, **Application Set**, and **Traffic Class** from the drop-down list.
- Step 6** Click **Import**.
- Step 7** Click the **Applications** tab and choose **Show > Discovered** to view the imported application.
-

Configure the NBAR Cloud Connector

The Application Visibility service uses the NBAR cloud connector to enrich the protocol pack and enhance visibility for unknown applications by sending and receiving data from the cloud.

- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
- Step 2** Click the **Discovered Applications** tab.
- Step 3** In the **NBAR Cloud** window, click **Configure**.
- Step 4** In the **Configure NBAR Cloud** window, click the toggle button to **Enable**.
- Step 5** Click the **Cisco API Console** link to retrieve the key and client secret.
- Step 6** Enter your Cisco credentials to open the **Cisco API Console** in a new browser tab and do the following:
- a) In the **My Apps & Keys** tab, click **Register a New App**.
 - b) Complete the following fields in the **Register an Application** screen.
 - **Name of Your Application**: Enter the application name.
 - **Application Type**: Check the **Service** check box.
 - **Grant Type**: Check the **Client Credentials** check box.
 - **Select APIs**: Check the **Hello API** check box.
 - c) Click **Register**.

The registered application details appear in the **My Apps & Keys** tab.

d) Copy the key and client secret of the registered application from the **Cisco API Console**.

Step 7 Complete the following fields in the **Configure NBAR Cloud** window:

- a) In the **Client ID** field, enter the key that you copied from the **My Apps & Keys** tab in the preceding step.
- b) In the **Client Secret** field, enter the client secret that you copied from the **My Apps & Keys** tab in the preceding step.
- c) In the **Organization Name** field, enter the organization name.
- d) Confirm that the **Enable Protocol Pack Auto Update** check box is checked. (It's checked by default.)
- e) Confirm that the **Improve my network using NBAR Cloud telemetry** check box is checked. (It's checked by default.)
- f) Under **NBAR classification telemetry data is being sent to region**, choose the desired location.

Step 8 Click **Save**.

Application Visibility Service Support for the Cisco DNA Traffic Telemetry Appliance

The Cisco DNA Traffic Telemetry Appliance generates endpoint telemetry from mirrored IP network traffic and shares the telemetry data with Cisco DNA Center for endpoint visibility and segmentation.

The prerequisites for enabling CBAR on the Cisco DNA Traffic Telemetry Appliance include:

- The device must be assigned to a site.
- The device role must be set to **Distribution** mode.

You can configure custom applications with attribute sets and maps on the Cisco DNA Traffic Telemetry Appliance without configuring a QoS policy. For more information, see [Create an Application Policy, on page 602](#) and [Deploy an Application Policy, on page 607](#).

Discover Infoblox Applications

You can integrate Cisco DNA Center with an organizational Infoblox DNS server to resolve unclassified traffic based on server names.

Before you begin

- The Infoblox WAPI version must be 1.5 or later. To check the Infoblox WAPI version, log in to the Infoblox server and choose **Help > Documentation > WAPI Documentation**.
- Create a role with at least Read Only permissions and assign the role to the Infoblox user. For more information, see Manage Users in the [Cisco DNA Center Administrator Guide](#).

Step 1 Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.

Step 2 Click the **Discovered Applications** tab.

Step 3 Under **Infoblox DNS Server**, click **Configure**.

Step 4 In the **Infoblox Connector Settings** window, click the **Here** link to configure IPAM/DNS server credentials in Cisco DNA Center.

- Step 5** Complete the IPAM settings. For more information, see [Configure an IP Address Manager in the Cisco DNA Center Administrator Guide](#).
- Step 6** Go back to **Infoblox Connector Settings** and complete the following settings:
- Check the **All DNS Zones** check box, or choose the required DNS zones from the **DNS Zones to Inspect** drop-down list. The drop-down list shows the DNS zones defined in the Infoblox server.
 - From the **Inspect** drop-down list, choose the required inspection record.
 - Check the **Read Application name from** check box and click the **Extensible Attribute** or **AVC RRTYPE format** radio button. If you click the **Extensible Attribute** radio button, enter the extensible attribute name that contains descriptive application names.
 - From **Default Traffic Class**, choose the default traffic class for classifying the Infoblox applications.
 - From **Default Application Set**, choose the default application set for classifying the Infoblox applications.
- Step 7** Click **Save**.
- The **Poll Infoblox to Import Applications** link appears under **Recommendations**.
- Step 8** Click the **Poll Infoblox to Import Applications** link to get a list of applications from the DNS zones configured in the **Infoblox Connector Settings**.
- Step 9** Choose the application that you want to import and complete the following:
- If the application does not have a name defined in the Infoblox server, edit the application name.
 - Choose the required application set and traffic class from the drop-down list if you want to change the default application set and traffic class defined in the **Infoblox Connector Settings**.
- Step 10** Click **Import**.
- Step 11** Click the **Applications** tab and choose **Discovered** in the **Show** drop-down list to view or edit the imported Infoblox applications.
- If you change the server name of an application after importing the application, the **Application Status** column in the **Infoblox Discovered Applications** window shows the status of the application as **Updated**. The application name that you see in the **Application Status** column is the new server name of the application. Click the info icon to view the old server names of the application.
-

Resolve Unclassified Traffic Using Microsoft Office 365 Cloud Connector

Cisco DNA Center can connect to external authoritative sources like Microsoft Office 365 Cloud Connector that can help classify the unclassified traffic or help generate improved signatures.


Before you begin

- Ensure that Cisco DNA Center has connectivity to the internet.
- Ensure that the NBAR cloud is enabled.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
- Step 2** Click the **Discovered Applications** tab.
- Step 3** Click the **MS Office 365 Cloud** toggle button to enable polling of MSFT signatures.
- When you enable Microsoft Office 365 Connector, the controller starts importing the new domains' information from Microsoft Office 365 and finds the correct application for the new domains.
 - The new secondary pack is installed along with the Cisco DNA Center-based protocol pack and new domains are supported automatically.
-

Edit or Delete a Discovered Application

If required, you can edit or delete a discovered application.

- Step 1** Click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
- Step 2** Click the **Application** tab.
- Step 3** Use the **Search**, **Show**, or **View By** fields to locate the discovered application that you want to change. You can search for applications based on their name, port number, and traffic class.
- Step 4** To edit the application:
- a) Click the application name and make the required changes.
For discovered applications, you can edit only the **Attribute Set** and **Traffic Class**.
 - b) Click **OK**.
- Step 5** To delete the application, click  in the application box, and then click **OK**.
-

Application Hosting

The following sections provide information about application hosting.

About Application Hosting

Application hosting lets you manage the lifecycle of third-party applications on devices managed by Cisco DNA Center. You can host third-party docker applications on Cisco Catalyst 9300 Series switches running Cisco IOS-XE software version 16.12.1s or later, Cisco Catalyst 9100 Series Access Points running Cisco IOS-XE software version 17.3.1 or later, and Cisco Catalyst 9400 Series switches running Cisco IOS-XE software version 17.1 or later.



Note The disk space allocated in Cisco DNA Center for the hosted applications is limited to 5 GB.

Install or Update the Application Hosting Service Package

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

-
- Step 1** Click the menu icon (☰) and choose **System > Software Updates**. Alternatively, click the cloud icon and click the **Go to Software Updates** link.
- Step 2** In the Software Updates window, review the following tabs:
- **Updates:** Shows the system and application updates. System Update shows the system version that is installed and the system updates that are available and have been downloaded from the Cisco cloud. Application Updates shows the available applications that can be downloaded and installed from the Cisco cloud, the size of the application, and the appropriate action (**Download**, **Install**, or **Update**). Hover your cursor over the package to view the available version and a basic description.
 - **Installed Apps:** Shows the application packages that are currently installed.
- Step 3** To download the Application Hosting package, click **Install** next to the Application Hosting name under **Updates > Application Updates**.
- Step 4** To update the Application Hosting package, click **Update** next to the Application Hosting name under **Updates > Application Updates**.
- Step 5** Ensure that the application has been updated by reviewing the version on the **Installed Apps** tab.

Note After installing the Application Hosting service package, you must log out of Cisco DNA Center, clear your browser cache, and log in to Cisco DNA Center again.

Prerequisites for Application Hosting

To enable application hosting on a Cisco Catalyst 9000 device, the following prerequisites must be fulfilled:

- Configure NETCONF port on the device before discovery.
- Configure a secure HTTP server on the switch where the applications will be hosted.
- Configure local or AAA authentication server for HTTPS user authentication on the switch. You must configure the username and password with privilege level 15.
- Ensure Cisco Catalyst 9300 Series switches are running Cisco IOS XE 16.12.x or later version and Cisco Catalyst 9400 Series switches are running Cisco IOS XE 17.1.x or later version.
- Ensure that the device has an external USB SSD pluggable storage (only for the switches of 9300 family).

- Verify that the configuration on the switch is correct. Open the WebUI on the switch and log in as the HTTPS user.

The following example shows a working configuration on a switch:

```
prompt# sh run | sec http
ip http server
ip http authentication local
ip http secure-server
ip http max-connections 16
ip http client source-interface Loopback0
```

Additional configuration for switches with a Cisco IOS XE release that is earlier than 17.3.3:

```
ip http secure-active-session-modules dnac
ip http session-module-list dnac NG_WEBUI
ip http active-session-modules none
```

Additional configuration for switches with Cisco IOS XE 17.3.3 or later:

```
ip http secure-active-session-modules webui
ip http session-module-list webui NG_WEBUI
ip http session-module-list pki OPENRESTY_PKI
ip http active-session-modules pki
```

- On Cisco DNA Center, configure the HTTPS credentials while manually adding the device. The HTTPS username, password, and port number are mandatory for application hosting. The default port number is 443. You can also edit the device credentials; see [Update Network Device Credentials, on page 78](#). If you edit a device that is already managed, resynchronize that device in the inventory before it is used for application hosting-related actions.



Note Application hosting HA is not supported on three-node Cisco DNA Center clusters.

View Device Readiness to Host an Application

You must check the readiness of the Cisco Catalyst 9300 Series switch to host the application before you can install an application on the switch.

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.
 - Step 2** Click **All Devices**.
 - Step 3** View the list of devices that are capable of hosting applications. The **App Hosting Status** indicates the readiness of the device to host an application. Click **See Details** to view the list of readiness checks performed on the device.
-

Add an Application

You can add a Cisco package or a docker application.

Before you begin

- **Cisco Package:** You must package the application using IOS SDK tools so that the application is compatible with IOS XE operating systems.
- **Docker:** You must save the docker image as a tar file. Enter the following command to store the docker image as a tar file:

```
docker save -o <path for generated tar file> <image name:tag>
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```

-
- Step 1** Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.
- Step 2** Click **New Application**.
- Step 3** Choose the application and category from the drop-down list.
- Step 4** Click **Select** and choose the application to upload.
- Step 5** Click **Upload**.
- You can view the newly added application in the **App Hosting** page.
-

Automatic Download of ThousandEyes Enterprise Agent Application

The ThousandEyes Enterprise Agent application lets you monitor your network and oversee the network traffic paths across internal, external, carrier, and internet networks in real time. The advantage of the ThousandEyes Enterprise Agent application is that you do not have to import this application manually in your Cisco DNA Center Application Hosting Service. When the switches and hubs in the network are enabled, the ThousandEyes Enterprise Agent application is downloaded automatically within 10 minutes of starting the Application Hosting Service. To manually download the application, click the following link to the ThousandEyes Enterprise Agent .tar file:

[thousandeyes-enterprise-agent.cat9k.tar](#)

If there is no internet connection, you can set a proxy connection from the console using the following command:

```
magctl service setenv app-hosting http_proxy <proxy-value>
```

Set the proxy value to connect to the ThousandEyes Enterprise Agent application.

Update an Application

You can update the application added in Cisco DNA Center.

- Step 1** Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.
You can view the available applications in the **App Hosting** window.
- Step 2** Choose the application that you want to update.
- Step 3** Click **Update App**.
- Step 4** Choose a new version of the application to be uploaded.

Step 5 Click **Upload**.

Start an Application

You can start an application in Cisco DNA Center.

- Step 1** Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.
 - Step 2** Choose the application and click **Manage** to view the devices that use the application.
 - Step 3** Choose the device that has the application that you want to start.
 - Step 4** From the **Actions** drop-down list, choose **Start App**.
-

Stop an Application

You can stop an application in Cisco DNA Center.

- Step 1** Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.
 - Step 2** Choose the application and click **Manage** to view the devices that use the application.
 - Step 3** Choose the device that has the application that you want to stop.
 - Step 4** From the **Actions** drop-down list, choose **Stop App**.
-

View Applications Hosted on Device

Before you begin

Complete the prerequisites. For more information, see [Prerequisites for Application Hosting](#).

- Step 1** Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.
- Step 2** To view all devices, click **All Devices** at the top-right corner, or to view only the devices that use a particular application, choose the application and click **Manage**.

If you chose to view all devices, the **All Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **IP Address**, **Image Version**, **App Hosting Status**, and **Last Updated**.

If you chose to view a list of devices for a particular application, the **Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **Device IP**, **App Version**, **App Status**, **Last Heard**, **Platform Version**, and **Action Status**.
- Step 3** In the **Devices** page, click **Summary** to view a summary of failed, stopped, and running applications on a device.
- Step 4** To take an action on an application, click the **Action** drop-down list and choose **Start**, **Stop**, **Edit**, **Upgrade**, or **Uninstall**.
- Step 5** Click the device link in which you want to view the installed hosting applications.

The **Applications** page shows the **Name**, **Version**, **App Status**, **Monitor App**, **Health**, and **Details** of the installed applications.

Note **Monitor App** contains the link to the Application Monitoring Dashboard. This link is provided in the, Cisco DNA Center application package controller, .yaml file. If this file does not contain application dashboard URL, then this **Monitor App** column will not be applicable.

Step 6 In the **Details** column, click **View** to get more information about an application status on the device. App details window shows the **RESOURCES**, **NETWORK**, and **DOCKER RUNTIME OPTIONS** information of an application.

Step 7 To download the log for a particular application, select the application and click **Application Logs**.

Step 8 To download tech support from the device, click **Tech Support Logs**.

Install an Application on a Cisco Catalyst 9300 Device

Cisco DNA Center allows you to install an application on a Cisco Catalyst 9300 Series switch.

Before you begin

- Complete the prerequisites. For more information, see [Prerequisites for Application Hosting, on page 530](#).
- Add the application to Cisco DNA Center. For more information, see [Add an Application, on page 531](#).
- Check the readiness of the switch to host the application. For more information, see [View Device Readiness to Host an Application, on page 531](#).

Step 1 Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.

Step 2 Choose the application and click **Install**.

Step 3 In the **Get Started** window, enter a unique name for your workflow in the **Task Name** field and click **Next**.

Step 4 In the **Select Site** window, choose the site where you want to enable the application, and click **Next**.

Step 5 In the **Select Switches** window, choose the devices on which you want to install the application and click **Next**.

You can choose the devices that are in **Ready** and **Partially Ready** status. Click **See Details** to view the list of readiness checks performed on the device.

For devices that are in **Partially Ready** status, click the **Check Now** link in the **Readiness Check** window to validate the HTTPS credentials.

If you don't find your device in the **Devices Table**, click **Import** to add devices from a CSV file.

Step 6 In the **Configuration App** window, complete the following settings:

- **Network Settings:**

- From the **Select Network** drop-down list, choose a VLAN to configure the application.
- From the **Address Type** drop-down list, choose **Static** or **Dynamic**. If you choose **Static**, click the thumbnail icon and enter the **IP Address**, **Gateway**, **Prefix/Mask**, and **DNS** for the application.

- **App Resources:** Check the **Allocate all resources available on a device** or the **Customize resource allocation** check box. You can check the **Customize resource allocation** check box and modify the maximum **CPU**, **Memory**, and **Persistent Storage** values to a lower value.
- **Custom Settings:** Applicable only for Cisco package applications. Enter the configuration details for the attributes that are specified by the application.
- **App Data:** Browse and upload the application-specific files. For information about how to identify the required application-specific files, see the relevant application document.
- **Docker Runtime Options:** Enter the docker runtime options required by the application.

Step 7 In the **Summary** window, review the application configuration settings.

Step 8 (Optional) Click **Configuration Preview** to view the configuration template used to push the configuration settings on the selected devices.

Step 9 Click **Provision**.

Step 10 In the confirmation window, click **Yes** to complete the application installation on the selected devices.

Note The installation of the application also modifies the Cisco IOS-XE configuration on the device. This change in the running configuration must be copied to the startup configuration to ensure applications function as expected after a router reload. After the application installation is complete, use the **Template Hub** to copy the running configuration to the startup configuration.

Uninstall an Application from a Cisco Catalyst 9300 Device

You can uninstall an application from a Cisco Catalyst 9300 Series switch.

Step 1 Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the devices that have the application that you want to uninstall.

Step 4 From the **Actions** drop-down list, choose **Uninstall App**.

Edit an Application Configuration in a Cisco Catalyst 9300 Device

You can edit an application configuration if the application requires a configuration to be up and running in a Cisco Catalyst 9300 Series switch.

Step 1 Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.

Step 2 Choose the application and click **Manage** to view the devices that use the application.

Step 3 Choose the device that has the application that you want to edit.

Step 4 From the **Actions** drop-down list, choose **Edit App Config**.

Delete an Application

You can delete an application from Cisco DNA Center.

Before you begin

You must uninstall the application from all devices that are using it. For more information, see [Uninstall an Application from a Cisco Catalyst 9300 Device, on page 535](#).

Step 1 Click the menu icon (☰) and choose **Provision > Services > App Hosting for Switches**.

You can view the available hosted applications in the **App Hosting** window.

Step 2 Choose the application that you want to delete.

Step 3 Click **Delete Application**.

Step 4 In the confirmation dialog box, click **OK**.

The application is deleted only if it is not used by any of the devices managed by Cisco DNA Center.

Otherwise, an error message shows the number of devices that are using the application. Click **Cancel** in the confirmation dialog box and uninstall the application. For more information, see [Uninstall an Application from a Cisco Catalyst 9300 Device, on page 535](#).

Download App Logs

You can download application logs from Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Provision > Services > IoT Services**.

Step 2 Click **All Devices**.

You can view the list of devices that are capable of hosting applications.

Step 3 Click **App logs** to download the application logs from Cisco DNA Center.

Step 4 In the **App Logs** pop-up window, choose the application logs file that you want to download and click **Download**.

Download Device Tech Support Logs

You can download the device tech support logs from Cisco DNA Center for troubleshooting purposes.

Step 1 Click the menu icon (☰) and choose **Provision > Services > IoT Services**.

Step 2 Click **All Devices**.

A list of devices that are capable of hosting applications is displayed.

Step 3 Click **Tech Support logs** to download the device tech support logs.

Application Hosting on Cisco Catalyst 9100 Series Access Points

The following sections provide information about application hosting on Cisco Catalyst 9100 Series Access Points.

About Application Hosting on Cisco Catalyst Access Points

The move to virtual environments has prompted the need to build applications that are reusable, portable, and scalable. Application hosting gives administrators a platform for leveraging their own tools and utilities. An application, hosted on a network device, can serve a variety of purposes. This ranges from automation, configuration management monitoring, and integration with existing tool chains.

Application hosting lets you manage the lifecycle of third-party applications on devices managed by Cisco DNA Center. This release lets you bring in the third-party SES-imagotag IoT Connector application on Cisco Catalyst 9100 Series Access Points with Cisco IOS-XE software version 17.3 or later.

The SES-imagotag IoT Connector on Cisco Catalyst 9100 Series Access Points can handle all Electronic Shelf Label (ESL) communication.

Application Hosting Workflow to Install and Manage USB on Cisco Catalyst 9100 Series Access Points

Before you begin

To enable application hosting on a device, the following prerequisites must be completed:

- Enable NETCONF and set the port to 830 to discover Cisco Catalyst 9100 Series Access Points.
- Make sure that the Cisco Catalyst 9100 Series Access Points have direct IP reachability to Cisco DNA Center.
- Make sure that the Cisco Catalyst 9800 Series Wireless Controller is running Cisco IOS XE 17.3.x or later software.
- Make sure that the Cisco DNA Center appliance is running the latest Cisco DNA Center ISO.
- Make sure that the USB dongle is inserted in the AP. This is required for the SES-imagotag Connector application to run.

Step 1 Check the readiness of the Cisco Catalyst 9800 Series Wireless Controller and Cisco Catalyst 9100 Series Access Points to host the application before you install it.

For more information, see [View Device Readiness to Host an Application, on page 531](#).

Step 2 Install the Application Hosting service on Cisco DNA Center.


For more information, see [Install or Update the Application Hosting Service Package, on page 530](#).

- Step 3** Add the Cisco Catalyst 9800 Series Wireless Controller to Cisco DNA Center.
For more information, see [Add a Network Device, on page 73](#).
- Note** Make sure that you enable NETCONF and set the port to 830.
You must wait for the Cisco Catalyst 9800 Series Wireless Controller to move to a Managed state.
- Step 4** Assign APs to a floor on the Network Hierarchy window.
For more information, see [Work with APs on a Floor Map, on page 146](#).
- Step 5** Upload the USB application (the SES-imagotag Connector) to Cisco DNA Center.
For more information, see [Add an Application, on page 531](#).
- Step 6** Enable the IoT services.
For more information, see [Enable IoT Services on Cisco Catalyst 9100 Series Access Points, on page 715](#).
- Step 7** Configure the container as described in the [Application Hosting on Catalyst APs Deployment Guide](#).
-

View Installed Hosting Applications on Cisco Catalyst 9100 Series Access Points

Before you begin

Make sure the prerequisites have been met. For more information, see [Prerequisites for Application Hosting](#).

- Step 1** Click the menu icon () and choose **Provision > Services > IoT Services**.
- Step 2** To view all devices, click **All Devices** at the top-right corner, or to view only the devices that use a particular application, choose the application and click **Manage**.
- If you chose to view all devices, the **All Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **IP Address**, **Image Version**, **App Hosting Status**, and **Last Updated**.
- Note** When the **App Hosting Status** of an AP is **Ready**, to configure the updates on the AP, check the check box next to the required hostname and click **Resync**.
- If you chose to view a list of devices for a particular application, the **Devices** page shows the following information about the devices that are capable of hosting applications: **Hostname**, **Device IP**, **App Version**, **App Status**, **Last Heard**, **Platform Version**, and **Action Status**.
- Step 3** In the **Devices** page, click **Summary** to view the summary of failed, stopped, and running applications on a device.
- Step 4** Click the **Action** drop-down list to start, stop, edit, upgrade, and uninstall an application.
- Step 5** Click the device link in which you want to view the installed hosting applications.
- The **Applications** page shows the **Name**, **Version**, **App Status**, **IP Address**, **Health**, and **Details** of the installed applications.
- Step 6** In the **Details** column, click **View** to get more information about an application status on the device.

App details window shows the **REOURCES** and **NETWORK** information of an application.

- Step 7** To download the application log, select an application for which you want to download the application log and click **Application Logs**.
- Step 8** To download the tech support log, select an application for which you want to download the tech support log and click **Tech Support Logs**.
-

Uninstall an Application from a Cisco Catalyst 9100 Device

You can uninstall an application from a Cisco Catalyst 9100 Series AP.

- Step 1** Click the menu icon (☰) and choose **Provision > Services > IoT Services**.
- Step 2** Choose the application and click **Manage** to view the devices that use it.
- Step 3** Choose the devices that have the application that you want to uninstall.
- Step 4** From the **Actions** drop-down list, choose **Uninstall App**.
-

Delete an Application from a Cisco Catalyst 9100 Device

You can delete an application from a Cisco Catalyst 9100 Series AP.

Before you begin

You must uninstall the application from all devices that are using it. For more information, see [Uninstall an Application from a Cisco Catalyst 9100 Device](#).

- Step 1** Click the menu icon (☰) and choose **Provision > Services > IoT Services**.
You can view the available hosted applications in the **IoT Services** page.
- Step 2** Choose the application that you want to delete.
- Step 3** Click **Delete Application**.
- Step 4** In the confirmation dialog box, click **OK**.
The application is deleted only if it is not used by any of the devices managed by Cisco DNA Center.
Otherwise, an error message shows the number of devices using the application. Click **Cancel** and uninstall the application.
For more information, see [Uninstall an Application from a Cisco Catalyst 9100 Device](#).
-

Configure a Site-to-Site VPN

You can create a site-to-site VPN and edit or delete existing site-to-site VPNs.

Create a Site-to-Site VPN

This procedure shows how to create a site-to-site VPN.

Before you begin

- Define the sites within the network hierarchy. See [Network Hierarchy Overview, on page 125](#).
- Configure IP address pools to be used for the VPN tunnels. The IP address pools must have a minimum of six free IP addresses. See [Configure IP Address Pools, on page 202](#).

-
- Step 1** Click the menu icon (☰) and choose **Provision > Site to Site VPN**.
Alternatively, you can create a site-to-site VPN from the **Workflows > Site to Site VPN** window.
- Step 2** To create a VPN, click **Add**.
The **Choose Your Sites** workflow is displayed.
- Step 3** In the **Choose Your Sites** workflow, do the following:
- a) Enter a VPN name in the first field.
 - b) Select the first site, a device in that site, and a WAN interface on that device from the Site 1 drop-down lists. The WAN interface is set by default if the device is provisioned.
 - c) Select the second site, a device in that site, and a WAN interface on that device from the Site 2 drop-down lists. The WAN interface is set by default if the device is provisioned.
- Step 4** In the **Select Networks** window, do the following:
- a) From the **Tunnel IP Pool** drop-down list, choose an IP address pool.
 - b) Check the boxes next to the subnets that you want to use for each site.
 - c) (Optional) If you want to add a custom network for a site, click the **Add Custom Networks** link at the bottom and complete the required fields.
- Step 5** In the **Configure VPN** window, do the following:
- a) Enter a preshared key for encryption.
 - b) Set the encryption and integrity algorithms as desired. We recommend that you use the default settings. If you change any settings, you can go back to the default choices by checking the **Use Cisco recommended IKEV2 & Transform Set Values** check box.
- Step 6** In the **Summary** window, review the VPN settings. To make any changes, click **Edit**.
- Step 7** To proceed, click **Create VPN**.
In the status screen that follows, a check mark is shown next to each step as it is completed. Click **Services** to return to the **Site to Site VPN** window, which shows the newly created VPN.
-

Edit a Site-to-Site VPN

-
- Step 1** Click the menu icon (☰) and choose **Provision > Site to Site VPN**.
- Step 2** Check the check box next to the VPN that you want to edit.

Step 3 Click **Edit** in the menu bar above the list.

Step 4 In the **Summary** window, review the VPN settings. To make any changes, click **Edit**.

Step 5 Click **Edit VPN** to submit the changes.

In the status screen that follows, a check mark is shown next to each step as it is completed. Click **Services** to return to the **Site to Site VPN** screen.

Delete a Site-to-Site VPN

Step 1 Click the menu icon (☰) and choose **Provision > Site to Site VPN**.

Step 2 Check the check box next to the VPN that you want to delete.

Step 3 Click **Delete** in the menu bar above the list.

A confirmation dialog box is displayed.

Step 4 Click **Yes** to confirm that you want to delete the VPN.

Create a User-Defined Network Service

Cisco DNA Center allows you to configure **Cisco User Defined Network** services from **Provision > Service Catalog > Cisco User Defined Network** page. Alternatively, you can create **Cisco User Defined Network** service from **Workflows > Configure Cisco UDN** page. For more information, see [Configure Cisco User-Defined Network](#).

View the User-Defined Network Service Provisioning Status

This procedure shows you how to view the Cisco User-Defined Network service provisioning status from the **Provision > All Services** window. You can also click the **View Provisioning Status** button in the **Configure Cisco User Defined Network** screen after configuring a Cisco User-Defined Network successfully.

Before you begin

Configure and provision the Cisco User-Defined Network service from the **Workflows > Configure Cisco User Defined Network** window.

Step 1 Click the menu icon (☰) and choose **Provision > All Services > Cisco User Defined Network**.

The **Site Provisioning Status** window displays the site name, device name, number of SSIDs used, and status of site provisioning.

Step 2 Click **Refresh** to see the latest provisioning status.

Step 3 Click the site name to view additional details for the provisioned device, such as SSID name, User-Defined Network (UDN) status, and Unicast Traffic Containment.

Step 4 Click **Activities** to track the scheduled task status in the **Scheduled Tasks** window.

Enable Telemetry on Switches

You can configure Switch Port Analyzer (SPAN) and Encapsulated Remote Switch Port Analyzer (ERSPAN) sessions on switches to share IP traffic for application assurance and endpoint analytics.

Before you begin

Confirm that the switches and the Traffic Telemetry Appliance (TTA) are reachable and managed through Cisco DNA Center. The switches must be assigned to a site and the **Distribution** device role.

Step 1 Click the menu icon (☰) and choose **Provision > Service Catalog > Telemetry Appliance Setup**.

Step 2 Click + **Setup** to create a new workflow.

Step 3 In the **Get Started** window, enter a workflow name and a description.

Step 4 In the **Choose Source Endpoint** window, choose a device to source traffic to a telemetry appliance.

Note Switches and hubs are the supported source devices for your workflow that is managed with the Distribution role.

Step 5 In the **Choose Destination Endpoint** window, choose the TTA device as the destination endpoint.

Note You can choose only one TTA device from the list.

Step 6 In the **Choose Type for Configuration** window, choose **SPAN** or **ERSPAN**.

Step 7 In the **Choose Mapping Between Source and Destination** window, do the following:

For SPAN:

- a. Choose the source interface on which to monitor incoming traffic.
- b. Choose the destination interface on the switch where the traffic telemetry appliance is connected and traffic can be forwarded.
- c. Choose the receiver interface to process the incoming traffic for analytics.

For ERSPAN:

- a. Choose the source interface on which to monitor incoming traffic.
- b. Enter the VLAN to filter the incoming traffic.
- c. Choose the receiver interface to process the incoming traffic for analytics.
- d. Enter the destination IP address for the receiver interface.
- e. Enter the destination netmask for the receiver interface.

Step 8 In the **Scheduler** window, click **Now** or **Later** to indicate when you want to start the configuration.

Step 9 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 10 To proceed, click **Deploy**.

Step 11 Click **View Status** to view the provisioning status of the individual devices.

Configure Cisco Umbrella

The following sections provide information about integrating Cisco Umbrella with Cisco DNA Center.

About Cisco Umbrella

The DNS-layer security in Cisco Umbrella provides the fastest and easiest way to improve your network security. It helps improve security visibility, detect compromised systems, and protect your users on and off the network by stopping threats over any port or protocol before they reach your network or endpoints.

Cisco DNA Center supports Cisco Umbrella configuration on the following devices:

- Cisco Catalyst 9800 Series Wireless Controllers with Cisco IOS-XE software version 16.12 or later
- Cisco Catalyst 9100 Series APs
- Cisco Catalyst 9200 Access Switch with Cisco IOS-XE software version 17.3.1 or later
- Cisco Catalyst 9300 Access Switch with Cisco IOS-XE software version 17.3.1 or later

Role-Based Access Control Settings for Cisco Umbrella

To configure Cisco Umbrella with Cisco DNA Center and to provision Cisco Umbrella on network devices, you must create a user role with the necessary RBAC permission for Cisco Umbrella. For more information, see "Manage Users" in the [Cisco DNA Center Administrator Guide](#).

Table 38: RBAC Permission Matrix for Cisco Umbrella

Function	Access	Permission
Configure Cisco Umbrella with Cisco DNA Center	Network Design > Advanced Network Settings	Write
Add Umbrella dashlet in System 360	Network Design > Advanced Network Settings	Write
Provision Cisco Umbrella on network devices	Network Provision > Provision	Write
	Network Design > Network Hierarchy	Read
	Network Provision > Inventory Management	Read
	System	Read
	Network Provision > Scheduler	Write
	Network Services > Umbrella	Write

Configure Cisco Umbrella with Cisco DNA Center

Before you begin

- Create a Cisco Umbrella account.
- Log in to *login.umbrella.com* and create the necessary keys, such as the API key, legacy token, management key, and secret.
- Note down the organization ID from the Cisco Umbrella login URL.
- Create the local bypass domains in Cisco Umbrella.
- If Cisco DNA Center has a proxy server configured as an intermediary between itself and the network devices it manages or the Cisco cloud from which it downloads software updates, you must configure access to the proxy server. For more information, see the Configure the Proxy section in the [Cisco DNA Center Administrator Guide](#).
- Install the Cisco Umbrella package in Cisco DNA Center. See the Download and Install Packages and Updates section in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with necessary RBAC permission for Cisco Umbrella. See [Role-Based Access Control Settings for Cisco Umbrella, on page 543](#).



Note You cannot install Cisco Umbrella package on a Cisco DNA Center cluster configured with IPv6.

Step 1 Click the menu icon (☰) and choose **System > Settings > External Services > Umbrella**.

Step 2 Enter the following details that you retrieved manually from Cisco Umbrella:

- **Organization ID**
- **Network Device Registration API Key**
- **Network Device Registration Secret**
- **Management API Key**
- **Management Secret**
- **Legacy Device Registration Token**

Step 3 Click **Save**.

Add the Umbrella Dashlet

You can add the **Umbrella** dashlet in the **System 360** page. The **Umbrella** dashlet shows the configuration status of Cisco Umbrella with Cisco DNA Center.

Before you begin

You must install the Cisco Umbrella package.

-
- Step 1** Click the menu icon (☰) and choose **System > System 360**.
- Step 2** From the **Actions** menu, choose **Edit Dashboard** and click **Add Dashlet**.
- Step 3** Choose **Umbrella Dashlet** and click **Add**.

The **Umbrella** dashlet appears under **Externally Connected Systems** in the **System 360** page. The **Umbrella** dashlet shows the status as **Available** and displays the organization ID, if Cisco Umbrella is configured with Cisco DNA Center.

If Cisco Umbrella is not configured with Cisco DNA Center, you can click the **Configure** link and complete the fields in **System > Settings > External Services > Umbrella**. See [Configure Cisco Umbrella with Cisco DNA Center, on page 544](#).

If the keys are changed in Cisco Umbrella, you can click the **Update** link and update the keys in **System > Settings > External Services > Umbrella**. See [Configure Cisco Umbrella with Cisco DNA Center, on page 544](#).

View the Umbrella Service Statistics Dashboard

Click the menu icon (☰) and choose **Provision > Services > Umbrella** to view the **Umbrella Service Stats** dashboard.

The dashboard displays the following dashlets:

- **Total Umbrella DNS Queries:** Shows the number of blocked DNS queries and allowed DNS queries for the selected site.
- **Blocked Umbrella DNS Queries:** Shows the number of DNS queries blocked by security policy and content policy for the selected site.

By default, the dashlet shows statistics for the last 3 hours. You can view statistics for the last 24 hours or 7 days by choosing the required time from the drop-down list in the top-left corner of the **Umbrella Service Stats** page.

Prerequisites for Provisioning Cisco Umbrella on Network Devices

Before provisioning Cisco Umbrella on network devices, ensure that:

- Cisco Umbrella is configured with Cisco DNA Center.
- Wireless provisioning is complete for the devices on which you want to provision Cisco Umbrella.
- The SSID configuration is nonfabric.
- The AP is provisioned, if the device is configured with a nonfabric SSID in FlexConnect mode.
- The device has direct internet access to establish connection with Cisco Umbrella.
- The Cisco Umbrella root certificate is available in the Cisco DNA Center trustpool. See [Configure Trustpool in the Cisco DNA Center Administrator Guide](#).

- If the device has a Cisco Umbrella configuration that is not set from Cisco DNA Center, remove the Cisco Umbrella configuration from the device and resync the device with Cisco DNA Center.

Provision Cisco Umbrella on Network Devices

Before you begin

Make sure the prerequisites have been met. For information, see [Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 545](#).



Note Cisco umbrella deployment on your organization's network can be monitored only from *login.umbrella.com*.

Step 1 Click the menu icon (☰) and choose **Workflows > Umbrella Deployment**.

Alternatively, do the following:

- Click the menu icon (☰) and choose **Provision > Umbrella**.
- Choose a site from the network hierarchy for which you want to deploy Cisco Umbrella.
- The **Select Devices** window appears. Go to Step 4 to continue the deployment workflow.

Step 2 If a task overview window appears, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window appears.

a) You can view the device readiness status in each site, as follows:

- **Eligible Devices:** Devices that are eligible for Cisco Umbrella configuration. See [Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 545](#).
- **Enabled Devices:** Devices that are already configured from Cisco DNA Center.

b) Choose a site to deploy and click **Next**.

Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella can be deployed on all child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 If you have chosen **Switches** in the **Select Device Type** window, do the following:

- a) In the **Select Devices** window, choose the wired device.
- b) In the **Configure Interface** window, do the following:
 1. Choose the ports you want to configure and click **Define Umbrella Interfaces**.
 2. In the **Select Configuration** dialog box, click the **Define Umbrella Interfaces** drop-down list and choose **IN(LAN)**, **OUT(WAN)** or **Disable Umbrella** and click **Save**.

Note You must choose at least one **IN** and one **OUT** interface to proceed further.

- c) In the **Define Umbrella Policy Mapping (Wired)** window, choose Umbrella policies at a global or interface level.
- d) In the **Configure Policies for Your Devices** window, choose the **IN(LAN)** interface and click **Define Umbrella Policies**.
- e) In the **Select Policy** dialog box, choose the policy for the selected interfaces and click **Save**.

Step 6

If you have chosen **Wireless Controllers** in the **Select Device Type** window, do the following:

- a) In the **Select Devices** window, choose the wireless device.
- b) Choose the SSIDs and select the required Cisco Umbrella policy for each SSID.

Note

- Only nonfabric SSIDs are listed on this page.
- If you choose an SSID and don't select the Cisco Umbrella policy, the default policy is mapped with the SSID.
- If you choose multiple policies, the order of enforcement of policies is defined in the Cisco Umbrella cloud portal.

- c) In the **Umbrella Policy Association (Wireless)** window, view the default policies applied to the SSIDs.

If you want to change the policies associated with the SSIDs, click the **Cisco Umbrella** link. In the Cisco Umbrella console, you can see the network identity after you have completed the deployment of Cisco Umbrella from Cisco DNA Center. For devices with Cisco IOS-XE software version 16.xx, the network identity is shown as global. For devices with a Cisco IOS-XE software version later than 16.xx, the network identity is shown as a custom name created based on the site and SSID name.

Step 7

In the **Review Internal Domains** window, add or delete the list of internal domains. The DNS queries that match a domain in the **Internal Domain** list are forwarded to the local DNS server instead of Cisco Umbrella.

Step 8

The **DNS Crypt** window appears. The **Enable DNS Packet Encryption** option is selected by default.

- a) In the **DNS Crypt** window, click **Next**.
- b) If you don't want DNS packet encryption, uncheck the **Enable DNS Packet Encryption** check box.

Step 9

In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 10

To proceed, click **Deploy**.

Step 11

In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 12

To proceed, click **Apply**.

Step 13

In the **Deployment** window, click **View Status** to view the deployment status in the **Scheduled Tasks** window.

You can view the Cisco Umbrella deployment status of the device and the device configuration status in Cisco Umbrella. You can also view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Disable Cisco Umbrella on Network Devices

Step 1

Click the menu icon (☰) and choose **Workflows > Umbrella Deployment**.

Alternately, do the following:

- Click the menu icon (☰) and choose **Provision > Services > Umbrella**.
- Choose a site from the network hierarchy from which you want to disable Cisco Umbrella.

- The **Select Devices** window appears. Go to Step 4 to continue the disable workflow.

Step 2 If a task overview window appears, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window appears.

a) You can view the device readiness status in each site, as follows:

- **Ready Devices:** Devices that meet the prerequisites for Cisco Umbrella configuration. See [Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 545](#).
- **Not Ready Devices:** Devices that do not meet the prerequisites.
- **Enabled Devices:** Devices that are already configured from Cisco DNA Center.

b) Choose the site that you want to disable, and click **Next**.

Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella is disabled on all the child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 In the **Select Devices** window, click the **Enabled** tab and choose the devices.

Step 6 Click the **Disable** radio button and choose the devices.

Step 7 In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 8 To proceed, click **Deploy**.

Step 9 In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 10 To proceed, click **Apply**.

Step 11 In the Deployment window, click **View Status** to view the deployment status in the **Scheduled Tasks** window.

You can view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Update the Cisco Umbrella Configuration on Network Devices

Step 1 Click the menu icon (☰) and choose **Workflows > Umbrella Deployment**.

Alternately, do the following:

- Click the menu icon (☰) and choose **Provision > Services > Umbrella**.
- Choose a site from the network hierarchy for which you want to update the Cisco Umbrella configuration.
- The **Select Devices** window appears. Go to Step 4 to continue the update workflow.

Step 2 If a task overview window appears, click **Let's Start** to go directly to the workflow.

Step 3 The **Choose Site** window appears.

a) You can view the device readiness status in each site, as follows:

- **Ready Devices:** Devices that meet the prerequisites for Cisco Umbrella configuration. See [Prerequisites for Provisioning Cisco Umbrella on Network Devices, on page 545](#).

- **Not Ready Devices:** Devices that do not meet the prerequisites.
- **Enabled Devices:** Devices that are already configured from Cisco DNA Center.

b) Choose the site that you want to update and click **Next**.

Note You can choose only one site at a time. If you choose a parent site, Cisco Umbrella is updated on all child sites at the same time.

Step 4 In the **Select Device Type** window, choose **Switches** or **Wireless Controllers**.

Step 5 If you have chosen **Switches** in the **Select Device Type** window, do the following:

- a) In the **Select Devices** window, choose the wired device and click the **Update** radio button.
- b) In the **Configure Interface** window, do the following:
 1. Choose the ports and click **Define Umbrella Interfaces**.
 2. In the **Select Configuration** dialog box, click the **Define Umbrella Interfaces** drop-down list and choose **IN(LAN)**, **OUT(WAN)** or **Disable Umbrella** and click **Save**.

Note You must choose at least one **IN** and one **OUT** interface to proceed further.

- c) In the **Define Umbrella Policy Mapping (Wired)** window, choose Umbrella policies at a global or interface level and click **Next**.
- d) In the **Configure Policies for Your Devices** window, choose the **IN(LAN)** interface and click **Define Umbrella Policies**.
- e) In the **Select Policy** dialog box, choose the policy for the selected interfaces and click **Save**.

Step 6 If you have chosen **Wireless Controllers** in the **Select Device Type** window, do the following:

- a) In the **Select Devices** window, choose the wireless device and click the **Update** radio button.
- b) In the **Define Umbrella Policy Map (Wireless)** window, choose the SSIDs and select the desired Cisco Umbrella policies to map, or unselect SSIDs to disable Cisco Umbrella.

Step 7 In the **Review Internal Domains** window, add or delete the list of internal domains. The DNS queries that match a domain in the **Internal Domain** list are forwarded to the local DNS server instead of Cisco Umbrella.

Step 8 The DNS Crypt window appears. The **Enable DNS Packet Encryption** option is selected by default. If you don't want DNS packet encryption, uncheck the **Enable DNS Packet Encryption** check box.

Step 9 In the **Summary** window, review the details. To make any changes, click **Edit**.

Step 10 To proceed, click **Deploy**.

Step 11 In the **Schedule** window, choose whether you want to deploy the configuration now or schedule it later.

Step 12 To proceed, click **Apply**.

Step 13 In the Deployment window, click **View Status** to view the deployment status in the **Scheduled Tasks** window. You can view the Cisco Umbrella deployment logs in the **Audit Logs** window.

Create Secure Tunnel

Cisco DNA Center allows the user to plan and deploy VPN Tunnels, which establishes secure connection between enterprise and branch location.



Note This feature is currently supported only on the Cisco Catalyst 9300X Series Switches.

Configure Secure Tunnel

You can use this procedure to plan and deploy secure tunnels in day N.


-
- Step 1** Click the menu icon (☰) and choose **Provision > Secure Tunnels**.
Alternatively, you can create a secure tunnel from the **Workflows > Create Secure Tunnel** window.
- Step 2** In the **Secure Tunnel** window, click **Create Secure Tunnel**.
- Step 3** If the task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 4** In the **Select Tunnel Type** window, choose the type of secure tunnel to create by clicking the **Site To Secure Access Service Edge (SIG/SASE)** tile.
This action creates a secure tunnel between the Cisco Catalyst 9300X Series switch and the Secure Internet Gateway.
- Step 5** In the **Select Secure Internet Gateway** window, click the drop-down list to choose the **Secure Internet Gateway**.
Do one of the following for the chosen Secure Internet Gateway:
- **Umbrella**: Ensure that you created a tunnel in Cisco Umbrella. You will need the tunnel ID and preshared key in the subsequent steps. For more information, see [Configure Cisco Umbrella with Cisco DNA Center, on page 544](#). If the tunnel is created in the Cisco Umbrella portal, check the confirmation check box.
 - **Zscaler**: Ensure that the tunnel is already created on the Zscaler portal. After you create the tunnel in Zscaler, the preshared key and the FQDN defined there are required to configure the tunnel parameters on the selected Cisco Catalyst 9300X Series switch. If the tunnel is created in the Zscaler portal, check the confirmation check box.
- Step 6** In the **Choose Site and Device** window, do the following for site and tunnel mapping:
- a. Choose the **Site** from the drop-down list.
 - b. Choose the **Device** from the drop-down list.
 - c. Choose the **Number of Tunnels** to create from the drop-down list.
 - d. For Zscaler, choose the **Tunnel Type** from the drop-down list.
 - e. Enter the **Tunnel Name**.
 - f. Choose the **Tunnel Source Interface**.
 - g. Check the check box if you want to use the same interface for the tunnel IP. If you do not want to use the same interface, uncheck the check box and choose the **Interface**.

h. Enter the **Data Center Location**.

Step 7 In **Define Tunnel Settings** window, do the following:

- a. For Umbrella, enter the **Pre-Shared Key (PSK)** for authentication.
- b. If the Secure Internet Gateway integration is not complete, do the following:
 1. Enter the **Tunnel ID** and choose one of the following:
 - a. **Fully Qualified Domain Name (FQDN)**: Use the **Tunnel ID** generated in Cisco Umbrella or the **User ID** generated in Zscaler.
 - b. **IP Address**: Use the IP address to which you want to connect.
- c. Check the check box to use the Cisco-recommended settings. To customize the values, uncheck the check box.

Step 8 In the **Configure Tunnel Traffic** window, choose from the following options to route the traffic:

- **Send all traffic**: To send all traffic through the IPsec tunnel to Umbrella.
- **Send Selected Traffic**: Enter the subnet and ingress interface for the subnet. You can add more subnets by clicking .

Step 9 In the **Schedule Task** window, choose whether you want to create the tunnel now or schedule it for later. Also, you can choose to **Generate CLI Preview**.

Step 10 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 11 Click **Create Secure Tunnel**.

The **Done!** window appears.

Step 12 Click the **View all Tunnels** tab to view the status of the tunnel creation.

This process might take some time. Click **Refresh**. When the tunnel is up, the status changes from Provision to Up.



PART VI

Configure Policies

- [Configure Group-Based Access Control Policies and Analytics, on page 555](#)
- [Configure IP-Based Access Control Policies, on page 583](#)
- [Configure Application Policies, on page 589](#)
- [Configure Traffic-Copy Policies, on page 617](#)



CHAPTER 23

Configure Group-Based Access Control Policies and Analytics

- [Group-Based Access Control](#), on page 555
- [Cisco Group-Based Policy Analytics](#), on page 568

Group-Based Access Control

Cisco DNA Center implements Software-Defined Access in two ways:

- Virtual networks (VNs) provide macro-level segmentation, such as to separate IoT devices from the corporate network.
- Group-based policies provide micro-level segmentation, such as to control what types of network traffic to permit or deny between engineering and HR groups.

Group-Based Access Control policies provide the following benefits:

- Rich identity-based access control functionality with network automation and assurance benefits.
- Granular access control.
- Security groups apply to all virtual networks, which simplifies policy management.
- Policy views help you to understand the overall policy structure, and create or update required access control policies.
- Eliminates the need to switch between different applications to manage security groups and define protected assets.
- Provides enhanced features for deploying enterprise-wide access control policies.
- Restricts lateral movement of threats like ransom ware before you have identity or Network Admission Control (NAC) applications in place.
- Provides an easy migration path to Cisco Identity Services Engine (Cisco ISE) for users who are using third-party identity applications, but want to move to Cisco ISE.

For information about creating IP pools, sites, and virtual networks in Cisco DNA Center, see the [Cisco DNA Center User Guide](#).

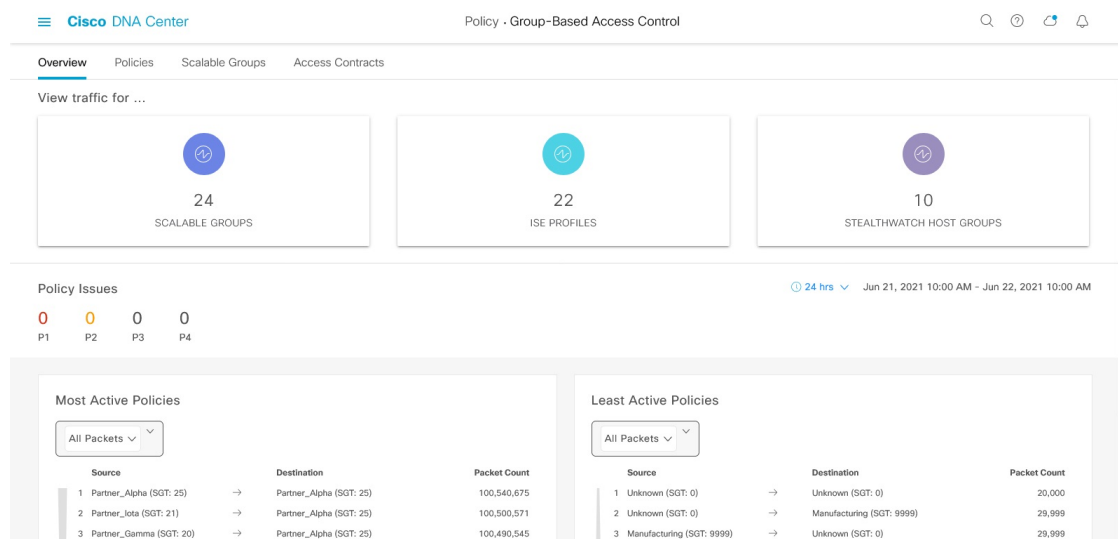
For information about configuring Cisco DNA Center for Cisco ISE, see the [Cisco DNA Center Installation Guide](#).

For information about configuring Cisco ISE for Cisco DNA Center, see the [Cisco Identity Services Engine Administrator Guide](#).

Group-Based Access Control Policy Dashboard

The Group-Based Access Control Policy dashboard provides you with a summary of network activity, policy-related issues, and traffic trends. Click the menu icon (☰) and choose **Policy > Group-Based Access Control > Overview** to view this dashboard.

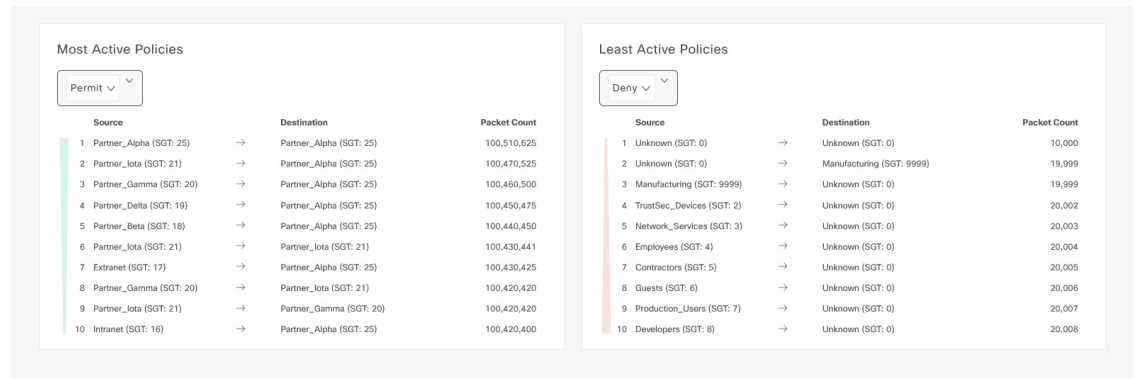
Figure 22: Group-Based Access Control Policy Dashboard



You can view the following details in this dashboard:

- **View Traffic:** You can view the traffic for security groups, Cisco ISE profiles, and stealthwatch host groups. You must install the Group-Based Policy Analytics package to view this data. Group-Based Policy Analytics provides you with insights to create group-based policies by visualizing communications between assets in order to assess the impact of introducing new access controls, and understand exactly which protocols you need to allow in the policies. Cisco Group-Based Policy Analytics aggregates information on groups of assets on your network, and their communication. For more information, see [Cisco Group-Based Policy Analytics, on page 568](#).
- **View Policy-Related Issues:** It displays a count of policy-related issues. Click a counter to view the details. It opens the **Assurance Issues** dashboard in a new browser tab, where you can view the details. Note that this view of policy-related issues is for the currently selected time period. Use the time selector to adjust the time window, as needed.
- **View Most Active and Least Active Policies:** It provides the details about the most active and least active policies. By default, this view is based on the count of total number of packets seen in the network for each policy (for each source-to-destination group pairing). You can use the drop-down list to select only the permitted packets or dropped packets. You can use the dropped packets option to see which policies are enforcing policy-based drops most actively.

Figure 23: Most and Least Active Policy Dashlets



Note that this view of policy activity is for the currently selected time period. Use the time selector to adjust the time window, as needed.

Group-Based Access Control Policies

Access control policies define which network traffic can pass from a source security group to a destination security group.

- **Security Group:** A classification category to which you can assign users, network devices, or resources. Security groups are used in access control policies. You can associate security groups with virtual networks based on your organization's network configuration, access requirements, and restrictions.
- **Contract:** An access contract is a set of rules that controls the type of network traffic that is allowed to pass between the source and destination security groups. In other words, a contract is a traffic filter definition. Access contracts define the actions (permit or deny) that are performed when the traffic matches a network application, protocol, and port. The default action is to use the catch all rule when no other rules match.
- **Group-Based Access Control Policies:** A group-based access control policy identifies a specific source and destination group pair and associates an access contract. The access contract specifies what types of traffic are permitted or denied between the source group and the destination group. These policies are unidirectional.

Security groups and access contracts are the basic building blocks of access control policy. While creating an access control policy, you can use the security groups and contracts that you have created earlier, or create new security groups and contracts while creating the policy. If you want to specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source and multiple destination groups. On the other hand, if you want to specify the source groups that are permitted to access a particular network resource, you can create an access control policy with a single destination and multiple source groups. For example, if you want to specify the network resources that can be accessed by the users associated with the Contractors source security group, you can create an access control policy with a single source and multiple destination groups. If you want to specify the source groups that are permitted to access the Finance Servers destination security group, you can create an access control policy with single destination and multiple source groups.

You can specify the default policy to be used when no contract is specified for a source and destination security group combination. The default policy is **Permit**. You can change this policy to **Deny**,

Permit_IP_Log, or **Deny_IP_Log**, if necessary. You can set the default policy based on your network type—an open or closed network.



Note We recommend that you change the default policy from **Permit** to **Deny** only if you have created explicit policies to permit necessary network traffic for all your network infrastructure devices. Failure to do so can result in loss of network connectivity.

List View

Click the **List** icon at the top-right corner of the **Group-Based Access Control** window to launch the **List** view.

- **Source View:** Displays a list of existing policies that are organized based on the source groups. You can expand each row to view the specific source-destination policy details.
- **Destination View:** Displays a list of existing policies that are organized based on the destination groups. You can expand each row to view the specific source-destination policy details.

To see which destination groups are available from a specific source group, use the **Source** view. To see which source groups are permitted to access a particular destination group, use the **Destination** view. For example, to see which destination groups are available to users who are part of the Contractors source security group, use the **Source** view. To see which source groups can access the Finance Servers destination security group, use the **Destination** view.

You can also view the policy enforcement statistics data in the policies listing table. The total number of permitted and denied policies are displayed for the selected time period.

The policy enforcement statistics are collected from the network devices that are provisioned for group-based policy and telemetry data language (TDL) subscription. These configurations are normally provisioned automatically for network devices that are part of a fabric. Manual configuration can be done for nonfabric network devices.

Note the following points while using the policy enforcement statistics data:

- Policy enforcement statistics data is available only when the Group-Based Policy Analytics package is deployed.
- Telemetry subscription is added as part of base provisioning for both fabric and nonfabric network devices. The TrustSec enforcement action is invoked when a new network device is added to Cisco DNA Center and assigned to a site.
- Software-Defined Access (SD-Access) adds TrustSec enforcement for the network devices that are added to a fabric. TrustSec telemetry data is collected only when this enforcement is enabled on a network device. If it is not enabled, the telemetry subscriptions used for policy monitoring are used to collect the TDL data for TrustSec.
- Cisco IOS XE 16.12 and later supports TDL streaming data.
- NETCONF must be enabled on the network devices.
- The following configuration must be added manually for the nonfabric network devices:

```
cts role-based enforcement vlan-list <VLAN of the endpoints>
```

- After upgrading, you will see the following message in the **Provision > Network Devices > Inventory** window:

We detected IOS-XE devices in your network where new telemetry subscription for assurance data needs to be enabled and some of the existing subscription needs to be optimized for performance. Please note that you will have to enable netconf and configure the netconf port in the Inventory credentials for these devices. Also note that these devices will receive a new subscription for group based policy monitoring telemetry. Do you want to take an action to provision these subscriptions?

Click **Apply Fix** to push the configuration to all the network devices with site assigned.

Matrix View

Click the **Grid** icon at the top-right corner of the **Group-Based Access Control** window to launch the Matrix view. The Matrix view is a core policy view that provides an overview of all the policies for all the security groups (whether explicit or default). You can use the Matrix view to view all the source and destination policies and understand the overall policy structure. You can view, create, and update access control policies from the Matrix view.

The Matrix view contains two axes:

- **Source axis:** The vertical axis lists all the source security groups.
- **Destination axis:** The horizontal axis lists all the destination security groups.

Place the cursor over a cell to view the policy for a given source security group and a destination security group. The color of a cell is based on the policy that applies to that cell. The following colors indicate which policies are applied to each cell:

- **Permit:** Green
- **Deny:** Red
- **Custom:** Gold
- **Default:** Gray

Place the cursor over the **Permit**, **Deny**, **Custom**, or **Default** icon that is displayed at the top of the matrix to view the cells to which the policy is applied.

The Matrix view highlights a cell and the corresponding row (source security group) and column (destination security group) when a cell is selected. The coordinates (source and destination security groups) of the selected cell are displayed near the matrix content area.

Click a cell to open the **Create Policy** or **Edit Policy** slide-in pane for that cell. The **Create Policy** slide-in pane shows the source and destination security groups as read-only fields. You can only update the policy status and access contract for that cell.

You can create custom views of the policy matrix to focus only on the policies that you are interested in. To do this, from the **View** drop-down list, choose **Create View**. While creating a custom view, you can specify the subset of the security groups that you want to include in the custom view. You can save the custom views and edit them later, if required. From the **View** drop-down list, choose **Manage Views** to create, edit, duplicate, or delete custom views. The **Default View** shows all the source and destination security groups.

You can navigate through the matrix by dragging the cursor over the matrix content area, or by using the horizontal and vertical scroll bars. You can also use the mini-map to navigate through the matrix. The mini-map

helps you to easily navigate through the matrix when the matrix size is large and extends beyond the screen size. You can move and place the mini-map anywhere on your screen. The mini-map provides the whole matrix view. The light gray portion in the mini-map represents the portion of the matrix that is currently displayed on your screen. You can drag your cursor over that area to scroll through the matrix.



Note The mini-map is closed by default. Click the **Expand** icon to expand and view the mini-map.

Use the **Filter** option to view a subset of the policy matrix for the selected set of source and destination groups. You can create a filter to focus only on the policies that you are interested in. To create the filter, select the source and destination groups that you want to include.

Policy Creation Overview

1. Define the categorizations for your organization or the portion of your organization that you plan to start with.
2. Create security groups for the categorizations that you identified.
3. Create access contracts for the types of network traffic that you wish to control. There are predefined sample access contracts to Permit or Deny all traffic, and also some example contracts showing more specific traffic filtering. You can create additional, more granular access contracts based on specific application definitions.
4. Decide which categories of network users require access to particular network resources, such as application servers and connections to other networks.
5. Create access policies, associate a source group, a destination group, and an access contract, to define how traffic is allowed to flow from the source to the destination.

Create a Security Group

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

- Step 1** Click the menu icon (☰) and choose **Policy > Group-Based Access Control > Security Groups**.
- Step 2** Click **Create Security Group**.
- Step 3** In the **Create Security Group** slide-in pane, enter a name and description (optional) for the security group.

Note The following characters are supported for the **Name** field:

- alphanumeric characters
- underscore (_)

The security group name must start with an alphabetic character.

Cisco DNA Center generates the tag value. You can update this value, if necessary. An error message is displayed if the value that you specified is already used by an existing security group. The valid range is from 2 to 65519.

Step 4 From the **Virtual Networks** drop-down list, choose the virtual networks to be associated with this security group. By default, the default virtual network is selected.

Note When Cisco DNA Center 2.3.3 or later is integrated with Cisco ISE 3.2 or later, security groups are not associated with virtual networks, and the **Virtual Networks** field is not displayed for these releases. However, if you are using Cisco ISE 3.1 or earlier, the security group and virtual network association details are displayed.

Step 5 Check the **Propagate to ACI** check box if you want the security group to be propagated to Cisco Application-Centric Infrastructure (ACI).

Step 6 Choose whether you want to create the security group now or schedule it for later.

If the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Cisco DNA Center, see the [Cisco DNA Center ITSM Integration Guide](#).

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Security Groups** window. Click the task status link to view the task details in **Activities > Tasks**. You can edit or cancel a task before it is executed.



Note You cannot create a security group with the name ANY or the tag value 0xFFFF/65535. Security Group ANY/65535 is a reserved internal security group that is used for the Cisco DNA Center default policy.

Edit a Security Group

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

Step 1 Click the menu icon (☰) and choose **Policy > Group-Based Access Control > Security Groups**.

Step 2 In the **Security Groups** window, check the check box next to the security group that you want to edit, and then click **Edit**.

Step 3 In the **Edit Security Group** slide-in pane, after making the necessary changes:


- Click **Save Now** to save the changes immediately.
- Click **Schedule Later** to schedule the update at a specific time. In the **Scheduler** slide-in pane, specify the start time, date, and time zone, and then click **Apply**.

When you update the security groups, you must deploy the changes on the network devices. Click **Deploy Now** to deploy the changes immediately, or click **Deploy Later** to deploy the changes later.

Delete a Security Group

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

-
- Step 1** Click the menu icon () and choose **Policy > Group-Based Access Control > Security Groups**.
- Step 2** Check the check box next to the security group that you want to delete.
- Step 3** Choose one of the following options:
- To delete the security group immediately, click **Delete Now**.
 - To delete the security group later, click **Delete Later**. In the **Schedule Delete** slide-in pane, specify the start time, date, and time zone, and then click **Apply**.



Note Click the link in the **Policies** column of a security group to view the access control rules using that security group and the policy to which it belongs. You cannot delete a security group if it is used in any access policy.

Synchronization of Security Groups Between Cisco DNA Center and Cisco ISE

While synchronizing the security groups in Cisco DNA Center with Cisco ISE:

- If a security group is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a security group is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If a security group name is the same in both Cisco DNA Center and Cisco ISE, but the description and ACI data are different, Cisco DNA Center is updated with the data specified in Cisco ISE.
- If a security group name is the same in Cisco DNA Center and Cisco ISE, but the tag values are different, a new security group with the tag value specified in Cisco ISE is created in Cisco DNA Center. The name of the existing security group in Cisco DNA Center is updated with the suffix **_DNAC**.
- If a tag value is the same but the security group name is different, the security group name in Cisco DNA Center is updated with the name specified in Cisco ISE.

An orange triangle icon is displayed next to a security group if synchronization with Cisco ISE is not completed.

Cisco ISE supports the packets coming from ACI to the TrustSec domain by synchronizing the Internal Endpoint Groups (IEPGs) and creating correlating read-only security groups in Cisco ISE. These security groups are displayed in the **Security Groups** window with the value **ACI** in the **Created In** column. You cannot edit or delete the security groups that are learned from ACI, but you can use them in the policies.

The **Associated Contracts** column shows the associated contracts for the security groups that are learned from ACI. Click the link displayed in the **Associated Contracts** column to view the details about the associated contracts.

When an IEPG is updated in ACI, the corresponding security group configuration is updated in Cisco ISE. A new EEPG is created in ACI when a security group is created in Cisco ISE.

Create an Access Contract

An access contract is a set of rules that controls the type of network traffic that is allowed to pass between the source and destination security groups. Access contracts define the actions (permit or deny) that are performed when the traffic matches a network application, protocol, and port.

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

Step 1 Click the menu icon (☰) and choose **Policy > Group-Based Access Control > Access Contracts**.

Step 2 Click **Create Access Contract**.

Step 3 In the **Create Access Contract** slide-in pane, enter the required details.

The **Modeled Access Contract** check box is enabled by default. This enables Cisco DNA Center to generate the valid commands for the underlying Security Group ACLs (SGACLs). When this option is enabled, the access contract is based on a model that allows you to create and edit without the need to know the underlying command line syntax.

Uncheck the **Modeled Access Contract** check box if you want to enter the SGACL command lines directly and store the access contract as text. Syntax checking is not done for the command line text that you enter. You must ensure that the command syntax is valid.

- Note**
- You can enable or disable this option only at the time of creating the access contracts. You cannot update this option for the existing access contracts.
 - Some of the advanced SGACL commands might not be supported on all Cisco network devices.

Step 4 Create the traffic filter rules:

- From the **Action** drop-down list, choose **Deny** or **Permit**.
- From the **Application** drop-down list, choose the application for which you want to apply that action. The port and protocol are automatically selected based on the application that you select.

If you want to specify the transport protocol, source port, and destination port, choose the **Advanced** option from the **Application** drop-down list.

You can create multiple rules. To create multiple rules for a contract, click the + symbol and choose the settings for the **Action** and **Application** columns. The rules are checked in the order in which they are listed in the contract. Use the handle icon at the left end of a rule to drag and change the order of the rule.

You can enable or disable logging for any traffic filter rule (including the default action) by using the **Logging** toggle. Logging is disabled by default. When logging is enabled, the network device sends a syslog message when the traffic filter rule is hit. This might be helpful in troubleshooting and initial testing of a policy. However, we recommend that you use this option sparingly because it might have a resource and performance impact on the network devices.

Step 5 From the **Default Action** drop-down list, choose **Deny** or **Permit**.

You can enable logging for the default action, if required.

Step 6 Choose whether you want to create the access contract now or schedule it for later.

If the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Cisco DNA Center, see the [Cisco DNA Center ITSM Integration Guide](#).

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Access Contract** window. Click the task status link to view the task details in **Activities > Tasks**. You can edit or cancel a task before it is executed.

Edit an Access Contract

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

-
- Step 1** Click the menu icon (☰) and choose **Policy > Group-Based Access Control > Access Contracts**.
 - Step 2** In the **Access Contracts** window, check the check box next to the access contract that you want to edit.
 - Step 3** Choose **Actions > Edit**.
 - Step 4** In the **Edit Access Contract** window, after making the necessary changes, choose whether you want to update the access contract now or schedule it for later.

You can use the **Filter** option to search for the contracts.

You can duplicate an existing access contract and create a new access contract by editing the required details. When you duplicate an access contract, all information in the existing access contract is copied and the copied contract has the existing contract name with the string **Copy** appended at the end. Click **Save Now** to create the duplicate contract immediately, or click **Schedule Later** to create the duplicate contract later.

When you update the security groups, contracts, or policies, you must deploy the changes on the network devices. If you update the policies and do not deploy the updated policies, notifications about the policy changes are not sent to the network devices, and the policies that are currently active in the network may not be consistent with the policy information displayed in Cisco DNA Center. To resolve this situation, you must deploy the updated policies on the network devices. Click **Deploy Now** to deploy the changes immediately, or click **Deploy Later** to deploy the changes later.

Cisco ISE provides the runtime policy platform for providing policy download to the network devices on behalf of Cisco DNA Center. The TrustSec Workcenter user interface screens for Security Groups, Security Group Access Control Lists (SGACLs), and Egress Policy are displayed in Read-Only mode in Cisco ISE to prevent policy synchronization issues.

Delete an Access Contract

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

-
- Step 1** Click the menu icon (☰) and choose **Policy > Group-Based Access Control > Access Contracts**.
- Step 2** In the **Access Contracts** window, check the check box next to the access contract that you want to delete, and then choose whether you want to delete the access contract now or schedule it for later.
-

You can view the sample contracts in the **Access Contracts** window. You can use or delete those sample contracts. However, you cannot delete the default contracts (Permit IP, Deny IP, Permit_IP_Log, and Deny_IP_Log).

Click the link in the **Policies** column of an access contract to view the policies that use that contract. You cannot delete a contract if it is used in a policy. You must delete the contract from that policy before you delete the contract.

Synchronization of Access Contracts Between Cisco DNA Center and Cisco ISE

While synchronizing the access contracts in Cisco DNA Center with Cisco ISE:

- If a contract is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a contract is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If a contract name is the same in Cisco DNA Center and Cisco ISE, but the description and traffic rule content are different, Cisco DNA Center is updated with the data specified in Cisco ISE.
- If the contract name and rule are the same, but the description is different, Cisco DNA Center is updated with the description specified in Cisco ISE.
- Text SGACL command lines in Cisco ISE are migrated as content that cannot be parsed. You can edit these contracts, but Cisco DNA Center does not parse them or check the syntax. The changes that you make in Cisco DNA Center are reflected in Cisco ISE.
- If a policy has multiple SGACLs in Cisco ISE, those contracts are migrated as default policies in Cisco DNA Center.

An orange triangle icon is displayed next to an access contract if synchronization with Cisco ISE is incomplete.

The contracts that are learned from ACI are displayed in the **Access Contracts** window with the value **ACI** in the **Created In** column. You cannot edit or delete the access contracts that are learned from ACI, but you can use them in the policies while using the ACI-learned security groups. While creating or updating a policy from the Matrix view, if you select an ACI-learned security group as the destination group, the associated access contracts are displayed in the **Preferred Contracts** tab. You can view all the access contracts in the **All Contracts** tab.

Create Group-Based Access Control Policy

Security groups and access contracts are the basic building blocks of an access control policy. While creating an access control policy, you can use the security groups and contracts that you have created before, or create new security groups and contracts while creating the policy.

To specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source and multiple destination groups. On the other hand, to specify the source groups that are permitted to access a particular network resource, you can create an access control policy with a single destination and multiple source groups.

For example, if you want to specify the network resources that can be accessed by the users associated with the *Contractors* source security group, you can create an access control policy with a single source and multiple destination groups. If you want to specify the source groups that are permitted to access the *Finance Servers* destination security group, you can create an access control policy with a single destination and multiple source groups.

Group-based access control policies can also be created or updated based on the traffic flows for a given source and destination group pair.

Step 1 In the **Policy List** or **Matrix** view, click **Create Policies**.

Step 2 To create an access control policy with a single source and multiple destination groups, click **Source to Destination(s)** and complete these steps:

- a) Click the radio button next to the source security group that you want to select.

If the security group that you want does not exist, click **Create Security Group** to create a new security group. This option is not available if the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled.

- b) Click **Next**.
- c) Choose the destination security groups to map to the selected source security group.

You can view the security group details and edit the security groups, if necessary.

Note If a policy already exists between the source and destination, an orange triangle icon is displayed near a security group.

- d) Click **Next**.
- e) Click the radio button next to the contract that you want to select. You can view and edit the contract details, if necessary.

If the contract that you want does not exist, click **Create Contract** to create a new contract. This option is not available if the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled.

Note You can choose only one contract for a policy.

- f) Click **Next**.

The **Summary** window lists the policies that are created based on the selected security groups and contract.

- g) Choose whether you want to create the policy now or schedule it for later.

Step 3 To create an access control policy with a single destination and multiple source groups, click **Destination to Source(s)** and complete the following steps:

- a) Click the radio button next to the destination security group that you want to select.

If the security group that you want does not exist, click **Create Security Group** to create a new security group. This option is not available if the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled.

- b) Click **Next**.
- c) Choose the source security groups to map to the selected destination security group.

You can view the security group details and edit the security groups, if necessary.

Note If a policy already exists between the source and destination, an orange triangle icon is displayed near a security group.

- d) Click **Next**.
- e) Click the radio button next to the contract that you want to select.

If the contract that you want does not exist, click **Create Contract** to create a new contract. This option is not available if the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled.

Note You can choose only one contract for a policy.

- f) Click **Next**.

The **Summary** window lists the policies that are created based on the selected security groups and contract.

- g) Choose whether you want to create the policy now or schedule it for later.

If the **Cisco DNA Center Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Cisco DNA Center, see the [Cisco DNA Center ITSM Integration Guide](#).

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Policies** window. Click the task status link to view the task details in **Activities > Tasks**. You can edit or cancel a task before it is executed.

Update a Group-Based Access Control Policy Based on Traffic Flows

Step 1 From the policy matrix view, click the cell for which you want to update the group-based access control policy.

Step 2 In the **Policy Details** slide-in pane, click **View Traffic Flows**.

In the **View Traffic Flows** slide-in pane, you can see the rules for the selected contract or the default policy in the left pane. You can view the traffic flows that match any selected rule in the right pane.

Step 3 Click **View Traffic** in the Default Action rule to see the list of flows that match that rule. While modifying an existing policy using access contracts with additional rules, use the **View Traffic** option for any rule to see the list of flows matching that rule.

For policies that are using the Default Action rule (with no explicitly selected access contract), you can select an access contract or create a new access contract to be used by that policy.

For policies with the access contract PERMIT or DENY, you can select an access contract or create a new access contract to be used by that policy.

For policies with the custom access contract, you can edit the selected access contract.

Step 4 After making the required changes, choose one of the following options:

- **Save the changes to the existing contract. Changes affect all the policies that reference the contract.**
- **Save the changes as a new contract. Changes are applied only to the current policy.**

- Save the changes as a new contract. Changes are not applied to any policy.
-

Synchronization of Policies Between Cisco DNA Center and Cisco ISE

While synchronizing the policies in Cisco DNA Center with Cisco ISE:

- If a policy is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a policy is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If a policy contract is different in Cisco ISE, Cisco DNA Center is updated with the contract specified in Cisco ISE.
- Policy mode information (Enabled, Disabled, or Monitor) is also imported from Cisco ISE.

Cisco ISE has an option to allow multiple SGACLs for a single policy (this option is not enabled by default in Cisco ISE). Cisco DNA Center does not support the use of multiple access contracts for a single policy. During policy synchronization, if a policy in Cisco ISE has multiple SGACLs, the Cisco DNA Center administrator is given the option to change that policy to have no contract selected (to use the default policy). The administrator can select a new or existing access contract for that policy after the policy synchronization is complete.

Cisco Group-Based Policy Analytics

About Cisco Group-Based Policy Analytics

Group-Based Policy Analytics enables you with insights, to create group-based policies by visualizing communications between assets, to assess the impact of introducing new access controls, and understand exactly which protocols you need to allow in the policies.

Cisco Group-Based Policy Analytics aggregates information on groups of assets on your network and their communication to answer the following questions:

- Which groups are communicating with each other?
- What kind of communication is this?
- Which group does a given asset belong to?

You can purchase one of following types of licenses for Cisco DNA Center:

- Cisco DNA Essentials
- Cisco DNA Advantage
- Cisco DNA Premier

Cisco DNA Advantage and Cisco DNA Premier contain the Group-Based Policy Analytics package. This package consists of the following archives (.tar.gz files):

- Backend
- User Interface
- Summarizer Pipeline
- Aggregation definitions

Install Group-Based Policy Analytics

Cisco Group-Based Policy Analytics is a part of Cisco DNA Center, but it is not installed by default.

To install Group-Based Policy Analytics, perform the following steps:

-
- Step 1** Click the menu icon (☰) and choose **System > Software Management**.
- Step 2** Scroll down to the **Available Applications for 2.3.x.x-xxxxx** area and select **Group-Based Policy Analytics**.
- Step 3** Click **Install** to install the application.
-

Hardware and Software Compatibility

Platform Support

Cisco Group-Based Policy Analytics is supported on the following hardware platforms:

- 44 cores, single node or three-node cluster
- 56 cores, single node or three-node cluster
- 112 cores, single node or three-node cluster

These platforms must meet the performance and scalability requirements mentioned here.

For details about the supported hardware, see [Cisco UCS M4 appliances](#) or [Cisco UCS M5 appliances](#).

The following table lists the performance metrics that Cisco DNA Center and Cisco Group-Based Policy Analytics support on each of the core platforms. The NetFlow metrics were introduced by Cisco Group-Based Policy Analytics.



Note The following table lists the performance metrics for a standalone deployment. These values might vary based on the number of nodes in the cluster and the number of installed packages.

Table 39: Performance Metrics

Metric	44 cores, three nodes	56 cores	112 cores
Devices (NADs)	5000 1000 switches or 1000 routers or a combination of both; 4000 APs	8000 2000 switches or 2000 routers or a combination of both; 6000 APs	18,000 5000 switches or 5000 routers or a combination of both; 13,000 APs

Metric	44 cores, three nodes	56 cores	112 cores
Clients (endpoints)	25,000 20,000 wireless; 5,000 wired	40,000 30,000 wireless; 10,000 wired	100,000 60,000 wireless; 40,000 wired
NetFlows per sec	30,000	48,000	120,000

Device Support

You must enable NetFlow to use Cisco Group-Based Policy Analytics. The following table shows the various ways in which NetFlow can be enabled on different network devices.

Table 40: Device Support

Network Devices	Series	NetFlow Configurable in telemetry section of Network Settings in Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Configurable using the template hub tool in the Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Collection in Fabric Deployment	NetFlow Collection in Nonfabric Deployment
Routers	Cisco 1000 Series Integrated Services Routers (ISR1K)	Yes	Yes	Yes	Yes
	Cisco 4000 Series Integrated Services Routers (ISR4K)	Yes	Yes	Yes	Yes
	Cisco Cloud Services Router 1000v Series (CSR 1000v)	Yes	Yes	Yes	Yes
	Cisco 1000 Series Aggregation Services Routers (ASR1K)	Yes	Yes	Yes	Yes

Network Devices	Series	NetFlow Configurable in telemetry section of Network Settings in Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Configurable using the template hub tool in the Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Collection in Fabric Deployment	NetFlow Collection in Nonfabric Deployment
Switches	Cisco Catalyst 9200 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9300 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9400 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9500 Series	No	Yes	Yes	Yes
	Cisco Catalyst 9600 Series	No	Yes	Yes	Yes
	Cisco Catalyst 2k Series	No	Yes	NA	Yes
	Cisco Catalyst 3560 Series	No	Yes	NA	Yes
	Cisco Catalyst 3650 Series	No	Yes	Yes	Yes
	Cisco Catalyst 3850 Series	No	Yes	Yes	Yes
	Cisco Catalyst 4k Series	No	Yes	Yes	Yes
	Cisco Catalyst 6500 Series Switches	No	Yes	Yes	Yes
	Cisco Catalyst 6800 Series Switches	No	Yes	Yes	Yes
Wireless Controllers	Cisco 3504 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco 5520 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco 8540 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco Catalyst 9800 Based Controller	Yes	Yes	Yes	Yes

Cisco ISE

Cisco ISE 2.4 Patch 7 and later, Cisco ISE 2.6 Patch 1 and later, and Cisco ISE 2.7 and later are supported.

Cisco Stealthwatch

Cisco Stealthwatch 7.x or later is supported.

Understand Connectors

Cisco Group-Based Policy Analytics gathers telemetry from the following sources, which are also known as connectors. You can configure the connectors either by following the [Initial Configuration of Cisco](#)

[Group-Based Policy Analytics, on page 572](#) workflow, or by choosing **Policy > Group-Based Access Control > Analytics > Configurations > Analytics Settings**.

Group Data Connectors

The group data connectors collect information about groups that assets are classified into. Cisco ISE and Cisco Stealthwatch are group data connectors.

- **Cisco ISE**

Cisco ISE is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE is installed on a virtual machine, a physical machine, or a combination of both. Cisco ISE uses the Cisco Platform Exchange Grid (pxGrid) service as the publisher-subscriber module for sharing Session Directory, security groups, and other information. PxGrid uses a query interface and supports bulk download. Users on the network are authenticated, authorized, and accounted for, and a Session Directory is maintained. User events are published to the connectors that are subscribed to the Session Directory service. Other services, like security group notifications, can also be subscribed to.

User identity and device information obtained during authentication is used to classify the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the network so that they can be properly identified for applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows Cisco ISE to enforce access control policies by enabling the network device to act upon the SGT to filter traffic.

In addition, Cisco ISE collects information about endpoints connected to your network, such as the type of device, OS, OS version, IP address and other attributes. These are called ISE profiles.

The Cisco ISE connector provides Cisco Group-Based Policy Analytics with SGT definitions and profiles from Cisco ISE.

- **Cisco Stealthwatch**

Cisco Stealthwatch is a network-based anomaly detection system that provides advanced threat detection, accelerated threat response, and network traffic security analysis. The Cisco Stealthwatch connector obtains the host groups that are configured on Cisco Stealthwatch. A host group is essentially a virtual container containing multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology.

Communication Connector


The communication connector helps gather information on traffic seen between groups that could be leveraged in Group-Based Policy decisions. This is done using NetFlow from network devices managed by Cisco DNA Center. NetFlow is collected and aggregated natively by Cisco DNA Center.

Initial Configuration of Cisco Group-Based Policy Analytics

This workflow helps you configure the data connectors that are required to collect telemetry data related to the network activity and endpoints from specific sources, such as Cisco ISE, Cisco Stealthwatch, and NetFlow. This task is useful when you are configuring the data connectors for the first time.

Before you begin

Cisco DNA Center must have Cisco Group-Based Policy Analytics installed.



-
- Step 1** Click the menu icon () and choose **Policy > Group-Based Access Control > Overview**. The **Create policies with more confidence** window is displayed.
- Step 2** Click **Get Started**.
The **Configure your data connectors** window is displayed.
- Step 3** Click **Let's Do It**.
The **Configure Group Data Connectors** window is displayed.
- Note** If the Cisco ISE version is earlier than the version required for running Cisco Group-Based Policy Analytics, an error message is displayed.
- Step 4** Click **Configure** at the bottom of the connector that you want to configure.
A new window opens, redirecting you to the Cisco DNA Center **Settings** window, where you can configure the required connectors. You must configure the Cisco ISE connector. Configuring the Cisco Stealthwatch connector is optional.
- Step 5** Close the **Settings** window. You will see a green dot next to the **Configure** option for the successfully configured connectors in the **Configure Group Data connectors** window.
- Step 6** Click **Next**.
The **Configure Communication Connectors** window is displayed.
- Step 7** Configure the communication connector (NetFlow) by using one of the following options:
- Provision NetFlow on the Cisco DNA Center device interface manually.
 - Click **Template Hub** to configure NetFlow using the **Template Hub Tool** in Cisco DNA Center.
 - Click **Telemetry in Network Settings** to configure NetFlow in the telemetry section of network settings.
- Step 8** Click **Next**.
The **Summary** window displays the configuration details of the connectors.
- Step 9** Click **Done** to start discovering your groups and endpoints.
-

Explore Groups and Endpoints

The following section provides information about the different ways to visualize traffic between different groups.

Multiple Groups to Multiple Groups

When you click the number that is displayed in the **Security Groups** box in the **Overview** window, the **Explore Security Groups** window is displayed. In this window, you can see a summary of all the group-to-group communication among security groups. By default, the time range for this view is the last available 24 hours of data. Note that this is different from the time range mentioned in the **Overview** window, where it is set to the last 14 days. The chart shows the top 25 source security groups and their corresponding interactions, starting with the source security group with the highest number of unique flows within the given time period and so on.

Click the  icon to display the chart view or  to display the table view.

In the table view, if you click the **See destinations** link on a particular row, it opens a window showing all the destination security groups for the selected source security group and the unique flow count for each destination security group.

Click a source group to view the **Single Group to Multiple Groups** window.

When you hover your cursor over a link, the link is highlighted and a tooltip shows the number of unique traffic flows. Clicking the link takes you to the **Single Group to Single Group** window.

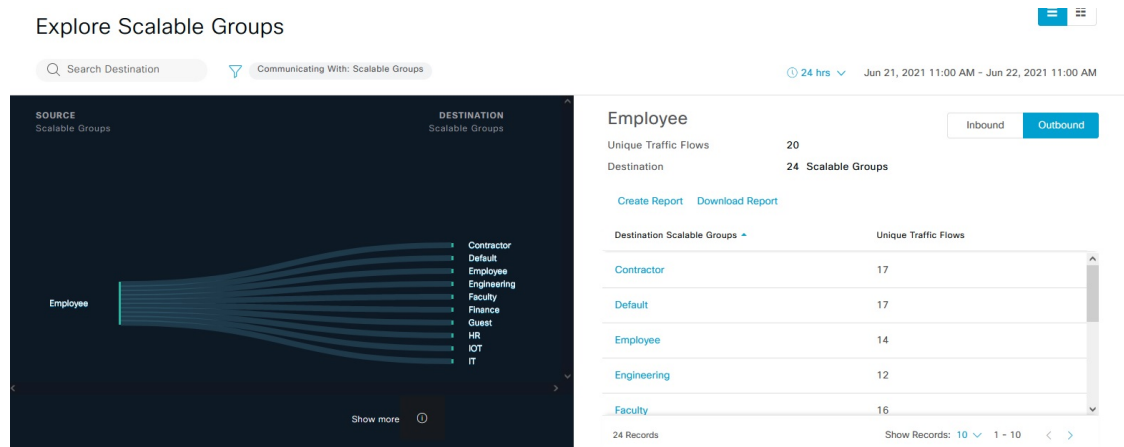
When you click the number displayed in the **ISE Profiles** box in the **Overview** window, the **Explore ISE Profiles** window is displayed. In this window, you can see a summary of all the communication from ISE Profiles as the source and security groups as the destination. In order to focus on the group-based policy decisions, either the source or destination category must be the security groups in this view.



When you click the number displayed in the **Stealthwatch Host Groups** box in the **Overview** window, the **Explore Stealthwatch Host Groups** window is displayed. In this window, you can see a summary of all the communication, with Stealthwatch Host Groups as the source and the security groups as the destination. In order to focus on the group-based policy decisions, either the source or destination category must be the security groups in this view.

Single Group to Multiple Groups

Single Group to Multiple Groups: Outbound

This window displays the activity between a single source group and multiple destination groups. The source or the destination or both must be a security group. By default, the time range for this view is the last available 24 hours of data, and the default number of links or records shown is 10.



Click the  icon to display the chart view or  to view the table view.

Outbound displays the connections initiated by the selected security group. **Inbound** displays the connections initiated by another group to this security group.

Click any column to sort it in ascending or descending order.

Click a group to view the **Single Group to Single Group** window with the corresponding destination as the selected group. The source group does not change.

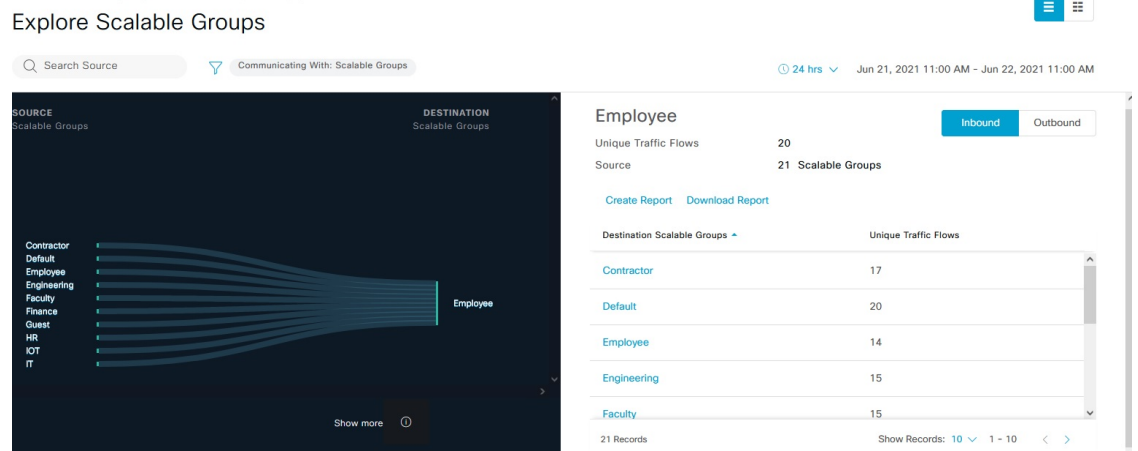
When you hover your cursor over a link, it is highlighted, and a tooltip shows the number of unique traffic flows. If you click this link, it takes you to the **Single Group to Single Group** window.

Click **Create Report** to generate a new report in CSV format with the information in this view. The **Reports** window opens, where you can see the generated report. This window also provides you access to previously generated reports and allows you to download the reports.

Click **Download Report** to view the generated reports. The **Reports** window opens, where you can click the *download* icon under the **Last Run** column to download a report.

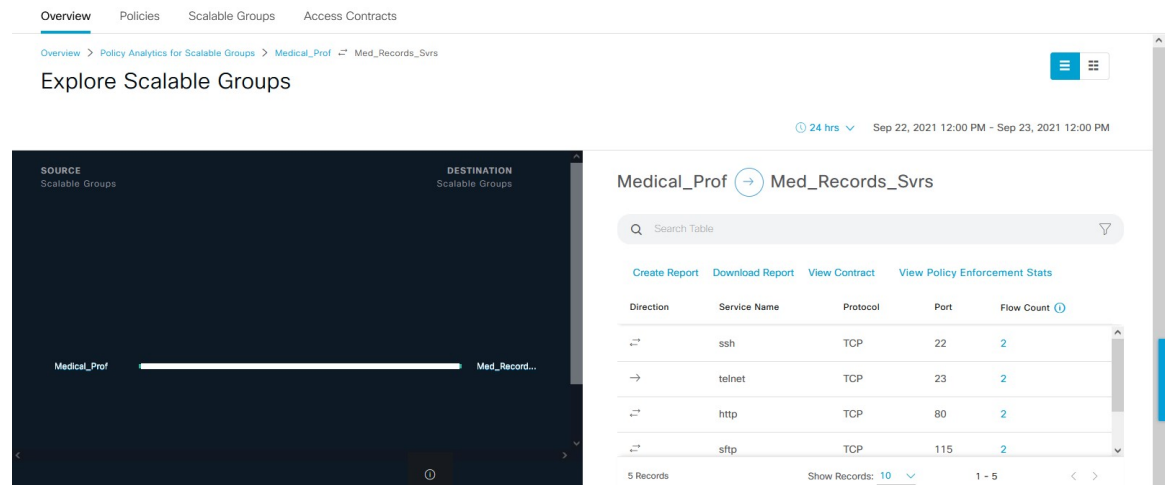
Single Group to Multiple Groups: Inbound

If you click **Inbound**, it shows all the connections initiated by any group as the source and the selected security group as the destination.



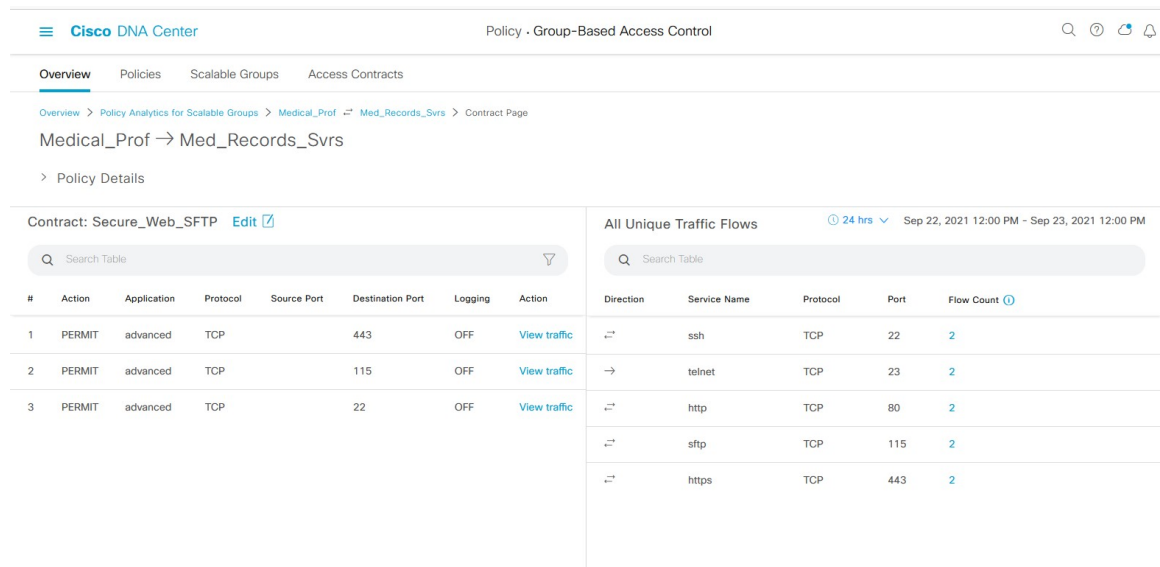
Single Group to Single Group

This window shows the activity between a source group and a destination group. Either the source group, the destination group, or both must be a security group. By default, the time range for this visual is the last available 24 hours of data, and the default number of links or records shown is 10.



When you click the directional arrow displayed between the source and destination groups, the source and destination groups are interchanged in this view.

Click **View Contract** to view a side-by-side comparison of traffic flows with the access contract rules that are in effect for this source and destination group pair.



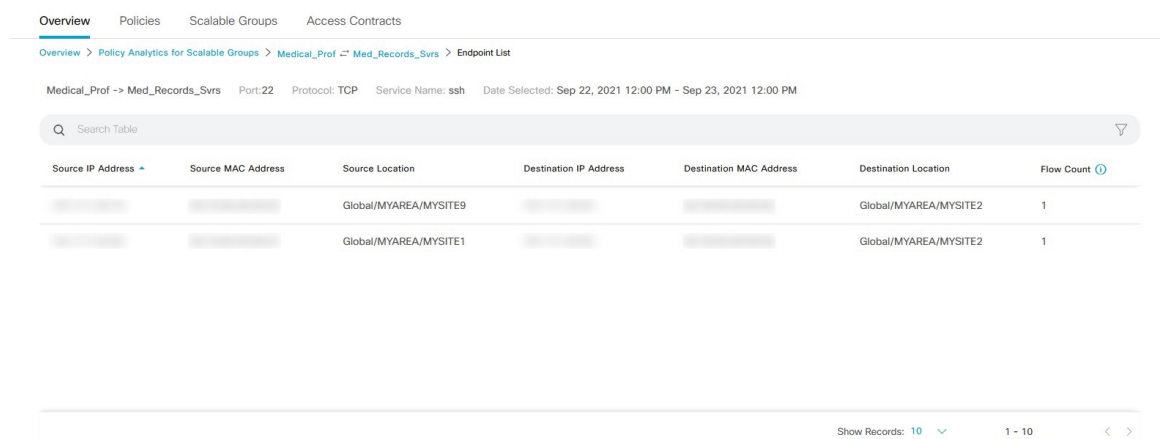
Contract: Secure_Web_SFTP [Edit](#)

#	Action	Application	Protocol	Source Port	Destination Port	Logging	Action
1	PERMIT	advanced	TCP		443	OFF	View traffic
2	PERMIT	advanced	TCP		115	OFF	View traffic
3	PERMIT	advanced	TCP		22	OFF	View traffic

All Unique Traffic Flows 24 hrs Sep 22, 2021 12:00 PM - Sep 23, 2021 12:00 PM

Direction	Service Name	Protocol	Port	Flow Count
↔	ssh	TCP	22	2
→	telnet	TCP	23	2
↔	http	TCP	80	2
↔	sftp	TCP	115	2
↔	https	TCP	443	2

The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane. You can view the flow direction, service name, flow count, ports, and protocol details in the right pane. The **Flow Count** column displays the number of flows detected for that particular service, port, and protocol combination for the selected time period. You can click the flow count link to view the flow details for each endpoint.



Medical_Prof -> Med_Records_Svrs Port: 22 Protocol: TCP Service Name: ssh Date Selected: Sep 22, 2021 12:00 PM - Sep 23, 2021 12:00 PM

Source IP Address	Source MAC Address	Source Location	Destination IP Address	Destination MAC Address	Destination Location	Flow Count
		Global/MYAREA/MYSITE9			Global/MYAREA/MYSITE2	1
		Global/MYAREA/MYSITE1			Global/MYAREA/MYSITE2	1

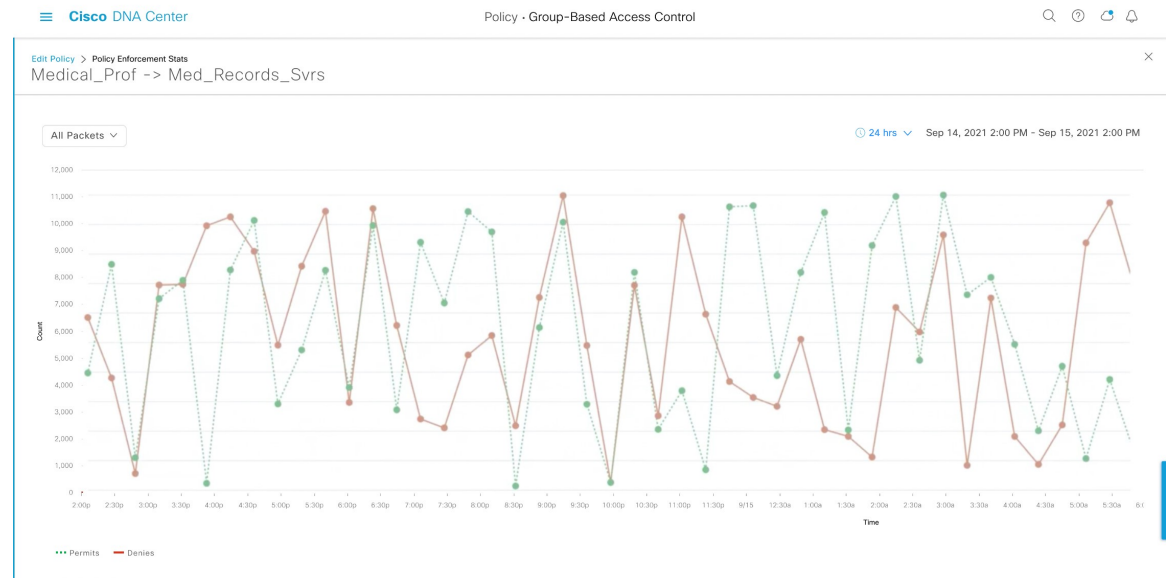
Show Records: 10 1 - 10



Note When you sort the **Traffic Flows** table based on the flow count, only 1000 records are displayed.



Click **View Policy Enforcement Stats** to view a time-series graph of the permit and deny counts for any source and destination group pair. It provides per-policy enforcement statistics visibility. You can use the **All**

Packets drop-down list to select only the permitted or dropped packets. Graph data points are displayed for each 15-minute data collection period. You can hover over any data point to view the number of permits and denials. You can click a data point or time period to view the contract and traffic flow details for the selected time period.



Note Note that the selected time period will be the hour that contains the 15-minute interval corresponding to the selected data point because the flow data aggregation is done every 60 minutes.

The **Traffic Flows** table can also be accessed from the **Policy Details** slide-in pane while creating or editing a policy.

Click the  icon to display the chart view or  to display the table view.

You can set the date and time using the [Date and Time Selector](#).

Click **Create Report** to generate a new report in CSV format with the information in this view. The **Reports** window opens, where you can see the generated report. This window also provides you access to previously generated reports and allows you to download the reports.

Click **Download Report** to view the generated reports. The **Reports** window opens, where you can click the *download* icon under the **Last Run** column to download a report.

Access Contracts

Access Contracts can now be created and modified directly in the Analytics workflow.

View Contract

To launch the **View Contract** window, from the **Explore Security Groups** window, click **View Contract**. The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane.

This table can also be accessed from the **Policies** window. Click the menu icon (☰) and choose **Policy > Group-Based Access Control > Policies**.

From the policy matrix view, click the cell for which you want to create or modify contracts. In the **Policy Details** slide-in pane, click **View Traffic Flows**.

If there is currently no contract assigned between the source and destination groups, no data is displayed. You can use the **Change Contract** or **Create Access Contract** option to create or modify the contract.

Click **View traffic** in the **Action** column to see the list of flows that match that rule.

Create Access Contract

To launch the **Contract Content** window, from the **Policy Details** pane, click **Create Access Contract**. To create the traffic filter rules:

1. From the **Action** drop-down list, choose **Deny** or **Permit**.
2. From the **Application** drop-down list, choose the application for which you want to apply that action. The port and protocol are automatically selected based on the application that you select.

If you want to specify the transport protocol, source port, and destination port, choose the **Advanced** option in the **Application** drop-down list.

You can create multiple rules. To create multiple rules for a contract, click the Plus icon and choose the settings for the **Action** and **Application** columns. The rules are checked in the order in which they are listed in the contract. Use the Handle icon at the left end of a rule to drag and change the order of the rule.

You can use the **Add to Contract** option within the **All Unique Traffic Flows** pane to add an entry to the contract.

While saving a newly created or edited contract, you have the following options:

- **Update current policy only:** A duplicate of the contract is created and applied to the current policy. Other policies that reference this contract are not affected.
- **Update contract for all referenced policies:** The contract is updated and applied to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected:** A duplicate of the contract is created but not applied to any policy.

Change Contract

To launch the **Change Contract** window, from the **Policy Details** pane, click **Change Contract**. All the available contracts are displayed. You can select the required contract and click **Change** to add that contract to the policy.

Edit Contract

The **Edit** option is displayed only when a contract has already been added to the policy. If you want to edit the contract details, click **Edit** displayed after the name of the contract.

After updating the contract, click **Save**. The following options are available:

- **Update current policy only:** A duplicate of the contract is created and applied to the current policy. Other policies that reference this contract are not affected.
- **Update contract for all referenced policies:** The contract is updated and applied to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected:** A duplicate of the contract is created but not applied to any policy.

After choosing the appropriate option, enter a name and description (if you select the first or third option), and then click **Confirm**.

Date and Time Selector

You can select the time period to specify the data in the connection summary. You can select a time range within the last 14 days up to the current hour.

Figure 24: Date and Time Selector

Select a time range within the last 14 days up to the current hour
(Mar 26, 2020 3:00 PM)

1 1 hour 12 hours 24 hours

Start Date	Start Time	End Date	End Time
3 / 25 / 2020	3:00 PM	Mar 26, 2020	3:00 PM

2 3

1. Select one of the options. The **End Time** will be adjusted automatically.
2. Specify the **Start Date** by entering the month, day, and year manually or by using the calendar icon.
3. Choose the **Start Time** from the drop-down menu.

Use Search

The **Overview** window has a **Search** field that can search across the data for security groups, ISE profiles, Stealthwatch host groups, IP addresses, or MAC addresses.

As you start entering the characters in the search field, an automatic search is performed for security groups, ISE profiles, and Stealthwatch host groups, and up to three results are displayed for each group type. For MAC addresses, the relevant characters are hexadecimal and colon.

Cisco Group-Based Policy Analytics supports both IPv4 and IPv6 addresses for endpoints. You can search and filter the endpoints using an IPv4 or IPv6 address.

- The following characters can be used to search and filter IPv4 addresses:

- Numbers (0-9)
- Dot (.)

You can enter up to 15 characters in the filter field.

- The following characters can be used to search and filter IPv6 addresses:

- Numbers (0-9)
- Lowercase and uppercase alphabetic characters (a-f, A-F)
- Colon (:)

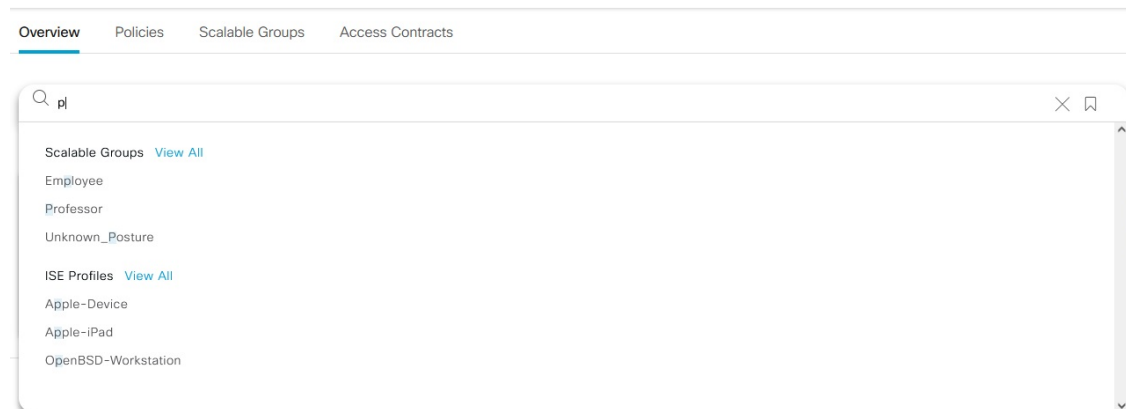
You can enter up to 39 characters in the filter field.



Note

- The **Search Results** window does not open until you click the **View All** link.
- A read-only user cannot search for an IP address or a MAC address. For more information, see [Role-Based Access Control, on page 581](#).

Figure 25: Search Window



From the **Focus** drop-down list, choose the required option to change your search criteria.

The filter icon is used in advanced filtering and is available only when you search for a MAC address or an IP address. When you click the filter icon, each column is provided with a search field on top of the column name.

For each column, you can enter up to three search criteria. When entering more than one criterion per column, you can specify an OR operation or an AND operation. The resultant query performs an AND operation across the columns.

Click the bookmark icon, and use the **Save Current Search** option to save the current displayed search.

To delete a saved search, click the bookmark icon. Hover your cursor over the name of the saved search, and click the cross icon. Click **Yes** in the **Delete Saved Filter** dialog box to permanently delete the filter.

Role-Based Access Control

Cisco Group-Based Policy Analytics supports Role-Based Access Control. It differentiates between a read-write user and a read-only user. However, because Cisco Group-Based Policy Analytics is primarily based on visibility, which does not make any changes to the system, there are only a few limitations for a read-only user:

- A read-only user cannot save search queries.
- A read-only user cannot configure the data connectors.
- A read-only user cannot export data because exporting data is an HTTPS POST operation.
- A read-only user can only perform a search by group and is restricted from other search functions because they involve HTTPS POST operations.



CHAPTER 24

Configure IP-Based Access Control Policies

- [IP-Based Access Control Policies, on page 583](#)
- [Workflow to Configure an IP-Based Access Control Policy, on page 584](#)
- [Configure Global Network Servers, on page 584](#)
- [Create an IP Network Group, on page 585](#)
- [Edit or Delete an IP Network Group, on page 585](#)
- [Create an IP-Based Access Control Contract, on page 585](#)
- [Edit or Delete an IP-Based Access Control Contract, on page 586](#)
- [Create an IP-Based Access Control Policy, on page 586](#)
- [Edit or Delete an IP-Based Access Control Policy, on page 588](#)
- [Deploy an IP-Based Access Control Policy, on page 588](#)

IP-Based Access Control Policies

An IP-based access control policy controls the traffic going into and coming out of a Cisco device in the same way that an Access Control List (ACL) does. As with an ACL, an IP-based access control policy contains lists of permit and deny conditions that are applied to traffic flows based on various criteria, including the protocol type, source IP address, destination IP address, or destination port number.

IP-based access control policies can be used to filter traffic for various purposes, including security, monitoring, route selection, and network address translation.

An IP-based access control policy has two main components:

- **IP Network Groups:** IP network groups comprise IP subnets that share the same access control requirements. These groups can be defined only in Cisco DNA Center. An IP network group may have as few as one IP subnet in it.
- **Access Contract:** An access contract is a common building block that is used in both IP-based and group-based access control policies. It defines the rules that make up the access control policies. These rules specify the actions (permit or deny) performed when traffic matches a specific port or protocol and the implicit actions (permit or deny) performed when no other rules match.

Workflow to Configure an IP-Based Access Control Policy

Before you begin

- Cisco ISE is not mandatory if you are adding groups within the **Policy > IP & URL Based Access Control > IP Network Groups** window while creating a new IP-based access control policy.
- Make sure that you have defined the following global network settings and provision the device:
 - Network servers, such as AAA, DHCP, and DNS servers. For more information, see [Configure Global Network Servers, on page 193](#).
 - Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see [Global Device Credentials Overview, on page 194](#).
 - IP address pools. For more information, see [Configure IP Address Pools, on page 202](#).
 - Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, see [Configure Global Wireless Settings, on page 207](#).

Step 1 Create IP network groups.

For more information, see [Create an IP Network Group, on page 585](#).

Step 2 Create an IP-based access control contract.

An IP-based access control contract defines a set of rules between the source and destination. These rules dictate the action (allow or deny) that network devices perform based on the traffic that matches the specified protocols or ports. For more information, see [Create an IP-Based Access Control Contract, on page 585](#).

Step 3 Create an IP-based access control policy. The access control policy defines the access control contract that governs traffic between the source and destination IP network groups.

For more information, see [Create an IP-Based Access Control Policy, on page 586](#).

Configure Global Network Servers

You can define the global network servers that become the default for your entire network.



Note You can override the global network settings on a site by the defining site-specific settings.

Step 1 Click the menu icon () and choose **Design > Network Settings > Network**.

Step 2 In the **DHCP Server** field, enter the IP address of a DHCP server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.
You must define at least one DHCP server in order to create IP address pools.

Step 3 In the **DNS Server** field, enter the domain name of a DNS server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.
You must define at least one DNS server in order to create IP address pools.

Step 4 Click **Save**.

Create an IP Network Group

Step 1 Click the menu icon (☰) and choose **Policy > IP & URL Based Access Control > IP Network Groups**.

Step 2 Click **Add Groups**.

Step 3 In the **Name** field, enter a name for the IP network group.

Step 4 In the **Description** field, enter a word or phrase that describes the IP network group.

Step 5 In the **IP Address or IP/CIDR** field, enter the IP addresses that make up the IP network group.

Step 6 Click **Save**.

Edit or Delete an IP Network Group

Step 1 Click the menu icon (☰) and choose **Policy > IP & URL Based Access Control > IP Network Groups**.

Step 2 In the **IP Network Groups** table, check the check box next to the group that you want to edit or delete.

Step 3 Do one of the following tasks:

- To make changes to the group, click **Edit**. For more information about field definitions, see [Create an IP Network Group, on page 585](#). Make the desired changes, and click **Save**.
 - To delete the group, click **Delete** and then click **Yes** to confirm.
-

Create an IP-Based Access Control Contract

Step 1 Click the menu icon (☰) and choose **Policy > IP & URL Based Access Control > Access Contract**.

Step 2 Click **Add Contract**.

Step 3 Enter a name and description for the contract.

- Step 4** From the **Implicit Action** drop-down list, choose either **Deny** or **Permit**.
- Step 5** From the **Action** drop-down list in the table, choose either **Deny** or **Permit**.
- Step 6** From the **Port/Protocol** drop-down list, choose a port or protocol.
- If Cisco DNA Center does not have the port or protocol that you need, click **Add Port/Protocol** to create your own.
 - In the **Name** field, enter a name for the port or protocol.
 - From the **Protocol** drop-down list, choose **UDP**, **TDP**, or **TCP/UDP**.
 - In the **Port Range** field, enter the port range.
 - If you want Cisco DNA Center to configure the port or protocol as defined, and not report any conflicts, check the **Ignore Conflict** check box.
 - Click **Save**.
- Step 7** (Optional) To include more rules in your contract, click **Add** and repeat Step 5 and Step 6.
- Step 8** Click **Save**.

Edit or Delete an IP-Based Access Control Contract

If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **IP Based Access Control Policies** window. A modified policy is considered to be stale because it is inconsistent with the policy that is deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

- Step 1** Click the menu icon (☰) and choose **Policy > IP & URL Based Access Control > Access Contract**.
- Step 2** Check the check box next to the contract that you want to edit or delete, and do one of the following tasks:
- To make changes to the contract, click **Edit**, make the changes, and click **Save**. For more information about field definitions, see [Create an IP-Based Access Control Contract, on page 585](#).
- Note** If you make changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy > IP & URL Based Access Control > IP & URL Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.
- To delete the contract, click **Delete**.

Create an IP-Based Access Control Policy

Create an IP-based access control policy to limit the traffic between IP network groups.

- Multiple rules can be added to a single policy with different configurations.
- For a given combination of IP groups and contract classifiers, rules are created and pushed to the devices. This count cannot exceed 64 rules as the Cisco Wireless Controller limits an ACL to have a maximum of 64 rules.

- If a custom contract or the IP group that is used in a **Deployed** policy is modified, the policy is flagged with the status as **Modified**, indicating that it is Stale and requires a redeployment for the new configurations to be pushed to the device.

Step 1 Click the menu icon (☰) and choose **Policy > IP & URL Based Access Control > IP & URL Access Control Policies**.

Step 2 Click **Add Policy**.

Step 3 Complete the following fields:

- Policy Name - Name of the Policy.
- Description - Word or phrase that identifies the policy.
- SSID - Lists FlexConnect SSIDs and non-FlexConnect SSIDs that were created during the design of SSIDs. If the selected SSID is configured in a FlexConnect mode, then the access policy is configured in a FlexConnect mode. Otherwise, it will be configured in a regular way.

Note If an SSID is part of one policy, that SSID will not be available for another policy.

A valid site-SSID combination is required for a policy deployment. You will not be able to deploy a policy if the selected SSID is not provisioned under any devices.

- Site Scope - Sites to which a policy is applied. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for an SSID, the policy is applied to all of the wireless devices with the SSID defined in the scope. For more information, see [Site Scope, on page 590](#).
- Source - Origin of the traffic that is affected by the contract. From the **Source** drop-down list, choose an IP network group. If the IP network that you want is not available, click **+Group** to create one.
- Contract - Rules that govern the network interaction between the source and destination in an ACL. Click **Add Contract** to define the contract for the policy. In the dialog box, click the radio button next to the contract that you want to use. Alternatively, you can select the permit (permit all traffic) or deny (deny all traffic) contract.
- Destination - Target of the traffic that is affected by the contract. Click the **Destination** drop-down list, choose an IP network group. If the IP network that you want is not available, click **+Create IP Network Group** to create one.
- Direction - Configures the relationship of the traffic flow between the source and destination. To enable the contract for traffic flowing from the source to the destination, select **One-Way**. To enable the contract for traffic flowing in both directions (from the source to the destination and from the destination to the source), select **Bi-directional**.

Step 4 (Optional) To create an IP network group, click **Create IP Network Group**.

Step 5 (Optional) To add another rule, click the plus sign.

Note To delete a rule, click **x**.

Step 6 (Optional) To reorder the sequence of the rules, drag and drop a rule in the order you want.

Step 7 Click **Deploy**.

The success message is displayed: IP-Based Access Control Policy has been created and deployed successfully. Depending on the SSID selected, either a FlexConnect policy or a standard policy is created with different levels of mapping information and deployed. The **Status** of the policy is shown as **DEPLOYED**. A wireless icon next to the **Policy Name** shows that the deployed access policy is a wireless policy.

Edit or Delete an IP-Based Access Control Policy

If you need to, you can change or delete an IP-based access control policy.



Note If you edit a policy, the policy's state changes to **MODIFIED** on the **IP Based Access Control Policies** window. A modified policy is considered to be stale because it is inconsistent with the policy that was deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

-
- Step 1** Click the menu icon (☰) and choose **Policy > IP & URL Based Access Control > IP & URL Access Control Policies**.
- Step 2** Check the check box next to the policy that you want to edit or delete, and do one of the following tasks:
- To make changes, click **Edit**. When you are done, click **Save**. For more information about field definitions, see [Create an IP-Based Access Control Policy, on page 586](#).
 - To delete the policy, click **Delete**.
- Step 3** If you make changes to the policy, deploy the modified policy by checking the check box next to the policy name and clicking **Deploy**.
-

Deploy an IP-Based Access Control Policy

If you make changes that affect a policy's configuration, you need to redeploy the policy to implement these changes.

-
- Step 1** Click the menu icon (☰) and choose **Policy > IP & URL Based Access Control > IP & URL Access Control Policies**.
- Step 2** Locate the policy that you want to deploy.
- Step 3** Check the check box next to the policy.
- Step 4** Click **Deploy**.
You are prompted to deploy your policy immediately or to schedule it for a later time.
- Step 5** Do one of the following:
- To deploy the policy immediately, click the **Run Now** radio button, and click **Apply**.
 - To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.



CHAPTER 25

Configure Application Policies

- [Application Policies Overview](#), on page 589
- [Manage Application Policies](#), on page 602
- [Manage Queuing Profiles](#), on page 612
- [Manage Application Policies for WAN Interfaces](#), on page 613

Application Policies Overview

Quality of Service (QoS) refers to the ability of a network to provide preferential or deferential service to selected network traffic. By configuring QoS, you can ensure that network traffic is handled in such a way that makes the most efficient use of network resources while still adhering to the objectives of the business, such as guaranteeing that voice quality meets enterprise standards, or ensuring a high Quality of Experience (QoE) for video.

You can configure QoS in your network using application policies in Cisco DNA Center. Application policies comprise these basic parameters:

- **Application Sets:** Sets of applications with similar network traffic needs. Each application set is assigned a business relevance group (business relevant, default, or business irrelevant) that defines the priority of its traffic. QoS parameters in each of the three groups are defined based on Cisco Validated Design (CVD). You can modify some of these parameters to more closely align with your objectives.
- **Site Scope:** Sites to which an application policy is applied. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope.

Cisco DNA Center takes all of these parameters and translates them into the proper device CLI commands. When you deploy the policy, Cisco DNA Center configures these commands on the devices defined in the site scope.



Note Cisco DNA Center configures QoS policies on devices based on the QoS feature set available on the device. For more information about a device's QoS implementation, see the corresponding device's product documentation.

CVD-Based Settings in Application Policies

The default QoS trust and queuing settings in application policies are based on the Cisco Validated Design (CVD) for Enterprise Medianet Quality of Service Design. CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by Cisco engineers to ensure faster, more reliable, and fully predictable deployment.

The latest validated designs relating to QoS are published in the Cisco Press book, *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition, available at: <http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694>. For additional information, see the following Cisco documentation:

- [Cisco Validated Designs](#)
- [Enterprise Medianet Quality of Service Design 4.0](#)
- [Medianet Campus QoS Design 4.0](#)
- [Medianet WAN Aggregation QoS Design 4.0](#)

Site Scope

A site scope defines the sites to which an application policy is applied. When defining a policy, you configure whether a policy is for wired or wireless devices. You also configure a site scope. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices in the site scope with the SSID defined in the scope.

This allows you to make tradeoffs as necessary to compensate for differences in the behaviors between wired and wireless network segments. For example, wireless networks typically have lower bandwidth, lower speed, and increased packet loss in comparison to wired networks. Individual wireless segments may exhibit further variation due to local conditions of RF interference, congestion, and other factors, such as the varying capabilities of network devices. The ability to apply per-segment policies to individual wireless segments enables the adjustment of traffic-handling rules to ensure that the highest-priority traffic is least affected by degradation of the wireless network.

Business-Relevance Groups

A business-relevance group classifies a given application set according to how relevant it is to your business and operations.

Business-relevance groups are Business Relevant, Default, and Business Irrelevant, and they essentially map to three types of traffic: high priority, neutral, and low priority.

- **Business Relevant:** (High-priority traffic) The applications in this group directly contribute to organizational objectives, and as such, may include a variety of applications, including voice, video, streaming, and collaborative multimedia applications, database applications, enterprise resource applications, email, file transfers, content distribution, and so on. Applications designated as business relevant are treated according to industry best-practice recommendations, as prescribed in Internet Engineering Task Force (IETF) RFC 4594.

- **Default:** (Neutral traffic) This group is intended for applications that may or may not be business relevant, for example, generic HTTP or HTTPS traffic may contribute to organizational objectives at times, while at other times, such traffic may not. You may not have insight into the purpose of some applications, for instance, legacy applications or even newly deployed applications. Therefore, the traffic flows for these applications should be treated with the Default Forwarding service, as described in IETF RFC 2747 and 4594.
- **Business Irrelevant:** (Low-priority traffic) This group is intended for applications that have been identified as having no contribution towards achieving organizational objectives. They are primarily consumer-oriented or entertainment-oriented or both in nature. We recommend that this type of traffic be treated as a *Scavenger* service, as described in IETF RFCs 3662 and 4594.

Applications are grouped into application sets and sorted into business-relevance groups. You can include an application set in a policy as-is, or you can modify it to meet the needs of your business objectives and your network configuration.

For example, YouTube is a member of the consumer-media application set, which is business-irrelevant (by default), because most customers typically classify this application this way. However, this classification may not be the true for all companies, for example, some businesses may be using YouTube for training purposes. In such cases, an administrator can move the YouTube application into the streaming-video application set, which is business relevant by default.

Consumers and Producers

You can configure relationships between applications such that when traffic from one application is sent to another application (thus creating a specific a-to-b traffic flow), the traffic is handled in a specific way. The applications in this relationship are called *producers* and *consumers*, and are defined as follows:

- **Producer:** Sender of the application traffic. For example, in a client/server architecture, the application server is considered the producer because the traffic primarily flows in the server-to-client direction. In the case of a peer-to-peer application, the remote peer is considered the producer.
- **Consumer:** Receiver of the application traffic. The consumer may be a client endpoint in a client/server architecture or it may be the local device in a peer-to-peer application. Consumers may be endpoint devices, but may, at times, be specific users of such devices (typically identified by IP addresses or specific subnets). There may also be times when an application is the consumer of another application's traffic flows.

Setting up this relationship allows you to configure specific service levels for traffic that matches this scenario.

Marking, Queuing, and Dropping Treatments

Cisco DNA Center bases its marking, queuing, and dropping treatments on IETF RFC 4594 and the business relevance category that you have assigned to the application. Cisco DNA Center assigns all of the applications in the Default category to the Default Forwarding application class and all of the applications in the Irrelevant Business category to the Scavenger application class. For applications in the Relevant Business category, Cisco DNA Center assigns traffic classes to applications based on the type of application. The following table lists the application classes and their treatments.

Table 41: Marking, Queuing, and Dropping Treatments

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Relevant	VoIP ⁵	Expedited Forwarding (EF)	Priority Queuing (PQ)	VoIP telephony (bearer-only) traffic; for example, Cisco IP phones.
	Broadcast Video	Class Selector (CS) 5	PQ	Broadcast TV, live events, video surveillance flows, and similar inelastic streaming media flows; for example, Cisco IP Video Surveillance and Cisco Enterprise TV. (Inelastic flows refer to flows that are highly drop sensitive and have no retransmission or flow-control capabilities or both.)
	Real-time Interactive	CS4	PQ	Inelastic high-definition interactive video applications and audio and video components of these applications; for example, Cisco TelePresence.
	Multimedia Conferencing	Assured Forwarding (AF) 41	Bandwidth (BW) Queue and Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED)	Desktop software multimedia collaboration applications and audio and video components of these applications; for example, Cisco Jabber and Cisco Webex.
	Multimedia Streaming	AF31	BW Queue and DSCP WRED	Video-on-Demand (VoD) streaming video flows and desktop virtualization applications, such as Cisco Digital Media System.
	Network Control	CS6	BW Queue only ⁶	Network control-plane traffic, which is required for reliable operation of the enterprise network, such as EIGRP, OSPF, BGP, HSRP, IKE, and so on.
	Signaling	CS3	BW Queue and DSCP	Control-plane traffic for the IP voice and video telephony infrastructure.
	Operations, Administration, and Management (OAM)	CS2	BW Queue and DSCP ⁷	Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on.
	Transactional Data (Low-Latency Data)	AF21	BW Queue and DSCP WRED	Interactive (foreground) data applications, such as enterprise resource planning (ERP), customer relationship management (CRM), and other database applications.
	Bulk Data (High-Throughput Data)	AF11	BW Queue and DSCP WRED	Noninteractive (background) data applications, such as email, file transfer protocol (FTP), and backup applications.

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Default	Default Forwarding (Best Effort)	DF	Default Queue and RED	Default applications and applications assigned to the default business-relevant group. Because only a small number of applications are assigned to priority, guaranteed bandwidth, or even to differential service classes, the vast majority of applications continue to default to this best-effort service.
Irrelevant	Scavenger	CS1	Minimum BW Queue (Deferential) and DSCP	Nonbusiness related traffic flows and applications assigned to the business-irrelevant group, such as data or media applications that are entertainment-oriented. Examples include YouTube, Netflix, iTunes, and Xbox Live.

⁵ VoIP signaling traffic is assigned to the Call Signaling class.

⁶ WRED is not be enabled on this class because network control traffic should not be dropped.

⁷ WRED is not enabled on this class because OAM traffic should not be dropped.

Service Provider Profiles

Service provider (SP) profiles define the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class models.

When application policies are deployed on the devices, each SP profile is assigned a certain service-level agreement (SLA) that maps each SP class to a DSCP value and a percentage of bandwidth allocation.

You can customize the DSCP values and the percentage of bandwidth allocation in a SP profile when configuring an application policy.

After you create the SP profile, you need to configure it on the WAN interfaces.

Table 42: Default SLA Attributes for SP Profiles with 4 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Default	0	—	—	31

Table 43: Default SLA Attributes for SP Profiles with 5 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Class 3 Data	AF11	—	—	1
Default	Best Effort	—	—	30

Table 44: Default SLA Attributes for SP Profiles with 6 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Class 1 Data	AF31	—	—	10
Class 3 Data	AF11	—	—	1
Video	AF41	—	—	34
Voice	EF	Yes	10	—
Default	0	—	—	30
Class 2 Data	AF21	—	—	25

Table 45: Default SLA Attributes for SP Profiles with 8 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Network-Control Management	CS6	—	—	5
Streaming Video	AF31	—	—	10
Call Signalling	CS3	—	—	4
Scavenger	CS1	—	—	1
Interactive Video	AF41	—	—	30
Voice	EF	Yes	10	—

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Default	0	—	—	25
Critical Data	AF21	—	—	25

Queuing Profiles

Queuing profiles allow you to define an interface's bandwidth allocation based on the interface speed and the traffic class.



Note Queuing profiles do not apply to WAN-facing interfaces that are connected to a service provider profile.

The following interface speeds are supported:

- 100 Gbps
- 10/40 Gbps
- 1 Gbps
- 100 Mbps
- 10 Mbps
- 1 Mbps

If the speed of an interface falls between two interface speeds, Cisco DNA Center treats the interface at the lower interface speed.



Note Cisco DNA Center attempts to detect the operational speed of the interface in order to apply the correct policy. However, if a switch port is administratively down, Cisco DNA Center cannot detect the speed. In this case, Cisco DNA Center uses the interface's supported speed.

You define a queuing policy as part of an application policy. When you deploy the application policy, the devices in the sites that are selected in the site scope are configured with the assigned LAN queuing policy. If no LAN queuing policy is assigned, the application policy uses the default CVD queuing policy.

If you change the queuing policy in an application policy that has already been deployed, the policy becomes stale, and you need to redeploy the policy for the changes to be configured on the devices.

Note the following additional guidelines and limitations of queuing policies:

- You cannot delete a LAN queuing profile if it is used in a policy.
- If you update a queuing profile that is associated with a policy, the policy is marked as stale. You need to redeploy the policy to provision the latest changes.

- Traffic class queuing customization does not affect interfaces on Cisco service provider switches and routers. You should continue to configure these interfaces without using Cisco DNA Center.

Table 46: Default CVD LAN Queuing Policy

Traffic Class	Default Bandwidth (Total = 100%) ⁸
Business Relevant Voice	10%
Business Relevant Broadcast Video	10%
Business Relevant Real-Time Interactive	13%
Business Relevant Multimedia Conferencing	10%
Business Relevant Multimedia Streaming	10%
Business Relevant Network control	3%
Business Relevant Signaling	2%
Business Relevant OAM	2%
Business Relevant Transactional Data	10%
Business Relevant Bulk Data	4%
Business Relevant Scavenger	1%
Business Relevant Best Effort	25%

⁸ We recommend that the total bandwidth for Voice, Broadcast Video, and Real-Time Interactive traffic classes equals no more than 33%.

Processing Order for Devices with Limited Resources

Some network devices have a limited memory (called TCAM) for storing network ACLs and access control entries (ACEs). So, because ACLs and ACEs for applications are configured on these devices, the available TCAM space is used. When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

To ensure that QoS policies for the most important applications get configured on these devices, Cisco DNA Center allocates TCAM space in the following order:

1. **Rank:** Number assigned to custom and favorite applications, but not to existing, default NBAR applications. The lower the rank number, the higher the priority. For example, an application with rank 1 has a higher priority than an application with rank 2, and so on. Having no rank is the lowest priority.



-
- Note**
- Custom applications are assigned rank 1 by default.
 - If we mark the NBAR application as favorite, the rank is set to 1000.
-

2. **Traffic Class:** Priority based on the following order: Signaling, Bulk Data, Network Control, Operations Administration Management (Ops Admin Mgmt), Transactional Data, Scavenger, Multimedia Streaming, Multimedia Conferencing, Real Time Interactive, Broadcast Video, and VoIP Telephony.
3. **Popularity:** Number (1–10) that is based on CVD criteria. The popularity number cannot be changed. An application with a popularity of 10 has a higher priority than an application with a popularity of 9, and so on.



Note

- Custom applications are assigned popularity 0.
- Default NBAR applications are assigned a popularity number (1–10) that is based on CVD criteria. When you mark an application as a favorite, this does not change the popularity number; only the rank is changed.

4. **Alphabetization:** If two or more applications have the same rank and popularity number, they are sorted alphabetically by the application’s name, and assigned a priority accordingly.

For example, let us assume that you define a policy that has the following applications:

- Custom application, custom_realtime, which has been assigned rank 1 and popularity 10 by default.
- Custom application, custom_salesforce, which has been assigned rank 1 and popularity 10 by default.
- Application named corba-iiop, which is in the transactional data traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 9 (based on CVD).
- Application named gss-http, which is in the Ops Admin Mgmt traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 10 (based on CVD).
- All other, default NBAR applications, which have no rank, but will be processed according to their traffic class and default popularity (based on CVD).

According to the prioritization rules, the applications are configured on the device in this order:

Application Configuration Order	Reason
1. Custom application, custom_realtime	Custom applications are given highest priority. Given that the custom_salesforce and custom_realtime applications have the same rank and popularity, they are sorted alphabetically, custom_realtime before custom_salesforce.
2. Custom application, custom_salesforce	
3. Favorite application, gss-http	Because both of these applications have been designated as favorites, they have the same application ranking. So, Cisco DNA Center evaluates them according to their traffic class. Because gss-http is in the Ops Admin Mgmt traffic class, it is processed first, followed by the corba-iiop application, which is in the Transactional Data traffic class. Their popularity does not come into play because the processing order has been determined by their traffic class.
4. Favorite application, corba-iiop	

Application Configuration Order	Reason
5. All other, default NBAR applications	All other applications are next and are prioritized according to traffic class and then popularity, with the applications having the same popularity being alphabetized according to the application's name.

Policy Drafts

When you create a policy, you can save it as a draft without having to deploy it. Saving it as a draft allows you to open the policy later and make changes to it. You can also make changes to a deployed policy, and save it as a draft.



Note After you save or deploy a policy, you cannot change its name.

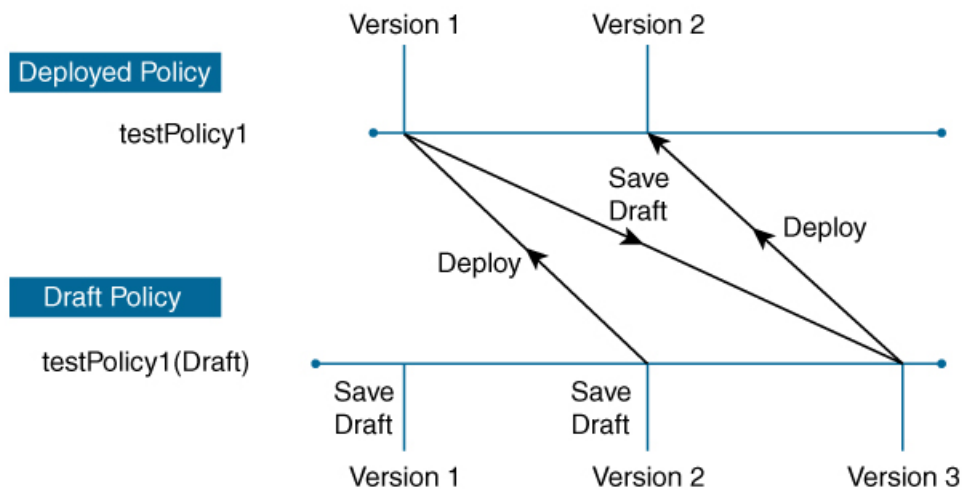
Draft policies and deployed policies are related to one another, but they have their own versioning.

When you save a policy as a draft, Cisco DNA Center appends the policy name with (Draft), and increments the version number. When you deploy a policy, Cisco DNA Center increments the version number of the deployed policy.

For example, as shown in the following figure, you create a policy named testPolicy1 and save it as a draft. The policy is saved as testPolicy1 (Draft), version number 1. You make a change to the draft and save it again. The policy has the same name, testPolicy1 (Draft), but its version number is incremented to 2.

You decide you like the policy, and you deploy it to the network. The policy is deployed with the name testPolicy1 and its version number is 1. You make a change to the deployed policy and save it as a draft. The draft policy, testPolicy1 (Draft), is incremented to version number 3. When you ultimately deploy that version, testPolicy1 is incremented to version 2.

Figure 26: Deployed Policy and Draft Policy Versioning



3555566

Any time you modify and save either a draft policy or a deployed policy, the draft policy version number is incremented. Similarly, any time you deploy either a draft policy or a modified deployed policy, the deployed policy version is incremented.

Just as with deployed policies, you can display the history of draft policies and roll them back to previous versions.

For more information about viewing the history of policy versions and rolling back to a previous version, see [Policy Versioning, on page 599](#).

Policy Preview

Before you deploy a policy, you can generate the CLI that will be applied to a device.

The Preview operation generates the CLI commands for a policy, compares them with the CLI commands in the running configuration on the device, and returns only the remaining CLI commands that are required to configure the policy on the device.

After reviewing the preview output, you can deploy the policy to all of the devices in the scope, or you can continue to make changes to the policy.

Policy Precheck

When you create an application policy, you can verify if it will be supported on the devices in the site scope before you deploy it. The precheck function verifies if the device type, model, line cards, and software images support the application policy that you created. If any of these components are not supported, Cisco DNA Center reports a failure for the device. Cisco DNA Center also provides possible ways to correct the failures. If these remedies do not fix the failure, you can remove the device from the site scope.

If you deploy the application policy as-is, the policy will fail to deploy on the devices that reported a failure during the precheck process. To avoid the failure, you can remove the device from the site scope or update the device components to a level that the application policy supports. For a list of supported devices, see the [Cisco DNA Center Compatibility Matrix](#).

Policy Scheduling

After you create or change a policy, you can deploy or redeploy the policy to the devices associated with it. You can deploy or redeploy a policy immediately or at a specific date and time, for example, on a weekend during off-peak hours. You can schedule a policy deployment for wired or wireless devices.

After you have scheduled a policy to be deployed, the policy and site scope are locked. You can view the policy, but you cannot edit it. If you change your mind about deploying the policy, you can cancel it.



Note When the scheduled event occurs, the policy is validated against the various policy components, for example, applications, application sets, and queuing profiles. If this validation fails, the policy changes are lost.

Policy Versioning

Policy versioning allows you to do the following tasks:

- Compare a previous version to the current (latest) one to see the differences.
- Display previous versions of a policy and select a version to reapply to the devices in a site scope.

Editing one version of a policy does not affect other versions of that policy or the components of the policy, such as the application sets that the policy manages. For example, deleting an application set from a policy does not delete the application set from Cisco DNA Center, other versions of that policy, or even other policies. Because policies and application sets exist independent of each other, it is possible to have a policy version that contains application sets that no longer exist. If you attempt to deploy or roll back to an older version of a policy that references an application set that no longer exists, an error occurs.



Note Policy versioning does not capture changes to applications (such as rank, port, and protocol), application set members, LAN queuing profiles, and sites.

Original Policy Restore

The first time that you deploy a policy to devices, Cisco DNA Center detaches the device's original Cisco Modular QoS CLI policy configurations, but leaves them on the device. Cisco DNA Center stores the device's original NBAR configurations in Cisco DNA Center. This allows you to restore the original Modular QoS CLI policies and NBAR configuration onto the devices later, if needed.



Note Because the Modular QoS CLI policies are not deleted from the device, if you remove these policies, you will not be able to restore them using the Cisco DNA Center original policy restore feature.

When you restore the original policy configuration onto a device, Cisco DNA Center removes the existing policy configuration that you deployed and reverts to the original configuration that was on the device.

Any Modular QoS CLI policy configurations that existed before you deployed application policies are reattached to the interfaces. However, queuing policies, such as multilayer switching (MLS) configurations, are not restored; instead, the devices retain the MLS configurations that were last applied through Cisco DNA Center.

After you restore the original policy configuration to the device, the policy that is stored in Cisco DNA Center is deleted.

Note the following additional guidelines and limitations for this feature:

- If the first attempt to deploy a policy to a device fails, Cisco DNA Center automatically attempts to restore the original policy configurations onto the devices.
- If a device is removed from an application policy after that policy has been applied to the device, the policy remains on the device. Cisco DNA Center does not automatically delete the policy or restore the QoS configuration on the device to its original (pre-Cisco DNA Center) configuration.

Stale Application Policies

An application policy can become stale if you change the configuration of something that is referenced in the policy. If an application policy becomes stale, you need to redeploy it for the changes to take affect.

An application policy can become stale for any of the following reasons:

- Change to applications referenced in an application set.
- Change to interfaces, such as SP Profile assignment, WAN subline rate, or WAN or LAN marking.
- Change to the queuing profile.
- New site added under a parent site in the policy.
- Device added to a site that is referenced by the policy.
- Devices moved between sites in the same policy.
- Change in interfaces exclusion/inclusion.
- Change in device Controller-Based Application Recognition (CBAR) status.

Application Policy Guidelines and Limitations

- Cisco DNA Center cannot learn multiple WLANs with the same SSID name on a wireless controller. At any point, Cisco DNA Center has only one entry for a WLAN with a unique name, although it is possible for the Cisco Wireless Controller to contain multiple entries with the same name and different WLAN profile names.

You might have duplicate SSID names per wireless controller by design, or you might have inadvertently added a wireless controller with a duplicate SSID name using Cisco DNA Center. In either case, having duplicate SSID names per wireless controller is problematic for several features:

- **Learn Config:** Cisco DNA Center learns only one randomly chosen SSID name per wireless controller and discards any remaining duplicate SSID names. (**Learn Config** is typically used in existing deployment scenario.)
 - **Application Policy:** When deploying an application policy, Cisco DNA Center randomly applies the policy to only one of the duplicate SSID names and not the others. In addition, policy restore, CLI preview, EasyQoS Fastlane, and PSK override features either fail or have unexpected outcomes.
 - **Multiscale Network:** In a multiscale network, multiple duplicate SSID names on multiple devices can cause issues. For example, one device has a WLAN configured as a nonfabric SSID, and a second device has the same WLAN, but it is configured as a fabric SSID. When you perform a **Learn Config**, only one SSID name is learned. The other SSID name from the other device is discarded. This behavior can cause conflicts, especially if the second device supports only fabric SSID names, but Cisco DNA Center is trying to perform operations on the device with nonfabric SSID names.
 - **IPACL Policy:** When deploying an IPACL policy, Cisco DNA Center randomly applies the policy to only one of the duplicate SSIDs. In addition, scenarios involving Flex Connect are also impacted.
- Cisco DNA Center does not recommend out-of-band (OOB) changes to device configurations. If you make OOB changes, the policy in Cisco DNA Center and the one configured on the device become inconsistent. The two policies remain inconsistent until you deploy the policy from Cisco DNA Center to the device again.
 - The QoS trust functionality cannot be changed.
 - Custom applications are not supported on the wireless controller. Therefore, custom applications are not selected while creating a wireless application policy.

- Make sure you delete the corresponding wireless application policy before deleting an SSID from design and reprovisioning the wireless controller.
- Wireless application for Cisco Catalyst 9800 Series Wireless Controller is not supported on SSID provisioned through learned configuration.
- Cisco DNA Center provides ACL-based Application Policy support for Cisco Catalyst IE 3300 Rugged Series switches and Cisco Catalyst IE 3400 Heavy Duty Series switches. You can deploy a maximum of eight port-based custom applications. However, there is no restriction for DSCP-based applications.



Note Cisco DNA Center does not support FlexConnect Local Switching mode for AireOS and Catalyst 9800 Series Wireless Controller platforms.

Manage Application Policies

The following sections provide information about how to manage application policies.

Prerequisites

To configure application policies, you must address the following requirements:

- Cisco DNA Center supports most Cisco LAN, WAN, and WLAN devices. To verify whether the devices and software versions in your network are supported, see the [Cisco DNA Center Compatibility Matrix](#).
- Make sure that your Cisco network devices, such as the ISR-G2, ASR 1000, and wireless controller, have the Application Visibility and Control (AVC) feature license installed. For information, see the [NBAR2 \(Next Generation NBAR\) Protocol Pack FAQ](#).
- AVC support is available for switches running Cisco IOS-XE 16.9 only if auto-QoS is not configured on the switches. You must upgrade the switches with auto-QoS to Cisco IOS-XE 16.11 or later to get AVC support.
- For Cisco DNA Center to identify the WAN interfaces that need policies, you must specify the interface type (WAN), and optionally, its subline rate and service-provider Class-of-Service model. For more information, see [Assign a Service Provider Profile to a WAN Interface, on page 614](#).
- Verify that the device roles that were assigned to devices during the discovery process are appropriate for your network. If necessary, change the device roles that are not appropriate. For more information, see [Change the Device Role \(Inventory\), on page 99](#).

Create an Application Policy

This section provides information about how to create an application policy.

Before you begin

- Define your business objectives. For example, your business objective might be to improve user productivity by minimizing network response times or to identify and deprioritize nonbusiness applications. Based on these objectives, decide which business relevance category your applications fall into.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.
- Verify that the device roles that were assigned to devices during the discovery process are appropriate for your network. If necessary, change the device roles that are not appropriate. For more information, see [Change the Device Role \(Inventory\)](#), on page 99.
- Add devices to sites. For more information, see [Add a Device to a Site](#), on page 90.
- If you plan to configure this policy with an SP profile for traffic that is destined for an SP, make sure that you have configured an SP profile. After creating the application policy, you can return to the SP profile and customize its SLA attributes and assign the SP profile to WAN interfaces. For more information, see [Configure Service Provider Profiles](#), on page 207.

Step 1 Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.

Step 2 Click **Add Policy**.

Step 3 In the **Application QoS Policy Name** field, enter a name for the policy.

Step 4 Click either the **Wired** or **Wireless** radio button.

Step 5 For wireless networks, select an SSID that is provisioned from the **SSID** drop-down list.

Step 6 Click **Site Scope** and check the check box next to the sites where you want to deploy the policy.

Note For policies of wired devices, you cannot select a site that is already assigned to another policy. For policies of wireless devices, you cannot select a site that is already assigned to another policy with the same SSID.

Step 7 For policies of wired devices, you can exclude devices or specific interfaces from being configured with the policy:

a) From the **Site Scope** pane, click the ellipsis icon (⋮) next to the site you are interested in.

A list of devices in the selected scope is displayed.

b) Locate the device that you want to exclude and click the toggle button in the corresponding **Policy Exclusions** column.

c) To exclude specific interfaces, click **Exclude Interfaces**.

d) From the list of **Applicable Interfaces**, click the toggle button next to the interfaces that you want to exclude.

By default, only the **Applicable Interfaces** are shown. You can choose **All** from the **Show** drop-down list to view all the interfaces.

e) Click < **Back to Devices in Site-Name**.

f) Click < **Back to Site Scope**.

Step 8 For WAN devices, you can configure specific interfaces:

a) From the **Site Scope** pane, click the ellipsis icon ⋮ next to the desired site.

b) From the list of devices in the site, click **Configure** in the **SP Profile Settings** column next to the desired device.

Note This option is only available for routers.

- c) In the **WAN Interface** column, from the **Select Interface** drop-down list, choose an interface.
 - d) In the **Role** column, from the **Select Role** drop-down list, choose a role according to the type of interface you are configuring:
 - Physical interface: Choose **WAN**. This role is the only valid role for a physical interface.
 - Tunnel interface: Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.
- Note** Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.

- e) In the **Service Provider Profile** column, from the **Select Profile** drop-down list, choose an SP profile.
- f) (Optional) If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.
- g) (Optional) To configure additional WAN interfaces, click + and repeat Step c through Step f.
- h) Click **Save**.
- i) Click < **Back to Site Scope**.

Step 9 From the **Site Scope** pane, click **OK**.


- Step 10** (Optional) If the CVD queuing profile (CVD_QUEUING_PROFILE) does not meet your needs, create a custom queuing profile.
- a) Click **Queuing Profiles**.
 - b) Select a queuing profile from the list in the left pane.
 - c) Click **Select**.

- Step 11** (Optional) If this policy is for traffic that is destined for an SP, customize the SP profile SLA attributes:
- a) Click **SP Profile**.
 - b) Choose an SP profile.
 - c) Customize the SLA attributes (**DSCP**, **SP Bandwidth %**, and **Queuing Bandwidth %**).

Step 12 (Optional) Configure the business relevance of the application sets used in your network.

Cisco DNA Center comes with application sets that are preconfigured into business-relevancy groups. You can keep this configuration or modify it by dragging and dropping an application set from one business-relevancy group to another.

Applications marked as a favorites are listed at the top of the application set. To change favorites, go to the Applications registry.

- Step 13** (Optional) Customize applications by creating consumers and assigning them to applications, or by marking an application as bidirectional:
- a) Expand the application group.
 - b) Click the gear icon  next to the desired application.
 - c) From the **Traffic Direction** area, click the **Unidirectional** or **Bi-directional** radio button.
 - d) To choose an existing consumer, from the **Consumer** drop-down list, choose the consumer that you want to configure. To create a new consumer, click + **Add Consumer** and define the **Consumer Name**, **IP/Subnet**, **Protocol**, and **Port/Range**.
 - e) Click **OK**.

Step 14 Configure host tracking. Click the **Host Tracking** toggle button to turn host tracking on or off.

When deploying an application policy, Cisco DNA Center automatically applies ACL entries to the switches to which collaboration endpoints (such as Telepresence units or Cisco phones) are connected.

The ACE matches the voice and video traffic generated by the collaboration endpoint, ensuring that the voice and video traffic are correctly marked.

When host tracking is turned on, Cisco DNA Center tracks the connectivity of the collaboration endpoints within the site scope and to automatically reconfigure the ACL entries when the collaboration endpoints connect to the network or move from one interface to another.

When host tracking is turned off, Cisco DNA Center does not automatically deploy policies to the devices when a collaboration endpoint moves or connects to a new interface. Instead, you need to redeploy the policy for the ACLs to be configured correctly for the collaboration endpoints.

Step 15 (Optional) Preview the CLI commands that will be sent to devices. For more information, see [Preview an Application Policy, on page 610](#).

Step 16 (Optional) Precheck the devices on which you plan to deploy the policy. For more information, see [Precheck an Application Policy, on page 611](#).

Step 17 Do one of the following tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see [Policy Drafts, on page 598](#).
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

To deploy the policy now, click the **Now** radio button and click **Apply**.

To schedule the policy deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment. For more information, see [Policy Scheduling, on page 599](#).

Note Site time zone setting is not supported for scheduling application policy deployments.

View Application Policy Information

You can display various information about the application policies that you have created and deployed.

Before you begin

You must have at least one deployed application policy.

Step 1 Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.

Step 2 Sort the policies by name, or filter them by name, status, or queuing profile.

Step 3 View the list of policies and the following information about each:

- **Policy Name:** Name of the policy.
- **Version:** Iteration of the policy. Each time a policy is deployed or saved as a draft, it is incremented by one version. For example, when you create a policy and deploy it, the policy is at version 1. If you change the policy and deploy it again, the version of the policy is incremented to version 2. For more information, see [Policy Drafts, on page 598](#) and [Policy Versioning, on page 599](#).
- **Policy Status:** State of the policy. If the policy is applied on Cisco Catalyst 3850, Catalyst 4500, and Catalyst 9000 devices and is impacted by the port channel update (create/modify/delete), an alert is shown in the policy status.

- **Deployment Status:** State of the last deployment (per device). Presents a summary of the following
 - Devices that were successfully provisioned.
 - Devices that failed to be provisioned.
 - Devices that were not provisioned due to the deployment being terminated.

Clicking the state of the last deployment displays the Policy Deployment window, which provides a filterable list of devices on which the policy is deployed. For each device, the following information is displayed:


- Device details (name, site, type, role, and IP address)
- Success deployment status. Clicking the gear icon next to the status launches the **Effective Marking Policy** window that shows the **Business Relevant** and **Business Irrelevant** applications and the traffic class queue in which they end up. For devices that have limited TCAM resources or an old NBAR protocol pack, only a subset of the applications that are included in the policy can be provisioned, and they are shown in the view.
- Failure status shows the reason for the failure.
- **Scope:** Number of sites (not devices) that are assigned to the policy. For policies of wireless devices, the name of the SSID to which the policy applies is included.
- **LAN Queuing Profile:** Name of the LAN queuing profile that is assigned to the policy.

Edit an Application Policy

You can edit an application policy.

Before you begin

You must have created at least one policy.

-
- Step 1** Click the menu icon () and choose **Policy > Application QoS > Application Policies**.
 - Step 2** Use the **Filter** field to locate the policy that you want to edit.
 - Step 3** Click the radio button next to corresponding policy.
 - Step 4** From the **Actions** drop-down list, choose **Edit**.
 - Step 5** Make changes to the application policy, as needed.
 - Step 6** You can change the business relevance of an application by moving application set between business relevant, business irrelevant, and default groups.
For information about the application policy settings, see [Create an Application Policy, on page 602](#).
 - Step 7** To update the queuing profile, click **Queuing Profiles**, and select a queuing profile from the list in the left pane.
 - Step 8** Click **Select**.
 - Step 9** Do one of the following tasks:
 - Save the policy as a draft by clicking **Save Draft**. For more information, see [Policy Drafts, on page 598](#).
 - Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

To deploy the policy now, click the **Run Now** radio button and click **Apply**.

To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see [Policy Scheduling, on page 599](#).

Note The site time zone setting is not supported for scheduling application policy deployments.

Save a Draft of an Application Policy

When creating, editing, or cloning a policy, you can save it as a draft so that you can continue to modify it later. You can also make changes to a deployed policy and save it as a draft.

Step 1 Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.

Step 2 Create, edit, or clone a policy.

Step 3 Click **Save Draft**.

For more information, see [Policy Drafts, on page 598](#).

Deploy an Application Policy

If you make changes that affect a policy's configuration, such as adding a new application or marking an application as a favorite, you must redeploy the policy to implement these changes.



Note Before deploying a policy, the Auto-QoS configuration is removed automatically from Cisco Catalyst 3650, Catalyst 3850, and Catalyst 9000 devices with Cisco IOS 16.x or later.

After creating custom applications, if CBAR is enabled for a device, the custom applications are configured automatically on the device. You must wait for the synchronization to the latest application registry to complete before deploying the application policy on the device. You can view the synchronization status in **Provision > Services > Service Catalog > Application Visibility**.

If CBAR is enabled for a device, while deploying the application policy, only the attribute sets and maps are configured on the device, because the custom applications are configured through CBAR.

Step 1 Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to deploy.

Step 3 Click the radio button next to the policy that you want to deploy.

Step 4 From the **Actions** drop-down list, choose **Deploy**.

a) If you redeploy the policy, you are prompted to take an appropriate action for the devices that were removed from the policy scope. Choose any one of the following actions:

- Delete policy from the devices (recommended)

- Remove devices from policy scope
- Remove devices from policy scope and restore devices to the existing configuration

b) Click **Apply**.

Step 5 You are prompted to deploy your policy now, or schedule it for later. Do one of the following:

- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
- To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

Cancel a Policy Deployment

After you click **Deploy**, Cisco DNA Center begins to configure the policy on the devices in the site scope. If you realize that you made a mistake, you can cancel the policy deployment.

The policy configuration process is performed as a batch process, in that it configures 40 devices at a time. If you have 40 devices or fewer and you cancel a policy deployment, your devices might be configured anyway, because the deployment to the first batch of devices would have already taken place. However, if you have hundreds of devices, canceling the policy deployment can be useful when needed.

When you click **Abort**, Cisco DNA Center cancels the configuration process on devices whose configuration has not yet started, and changes the device status to **Policy Aborted**. Cisco DNA Center does not cancel the deployments that are in the process of being completed or have been completed. These devices retain the updated policy configuration and reflect the state of the policy configuration, whether it is Configuring, Successful, or Failed.

During a policy deployment, click **Abort** to cancel the policy configuration process.

Delete an Application Policy

You can delete an application policy if it is no longer needed.

Deleting policy deletes class maps, policy map, and association of policy map with wireless policy profile.

Step 1 Click the menu icon () and choose **Policy > Application QoS > Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to delete.

Step 3 Click the radio button next to the policy that you want to delete.

Step 4 From the **Actions** drop-down list, choose **Undeploy Policy**.

Step 5 In the **Undeploy Policy** window, click the **Delete policy from devices** radio button and click **Apply**.

Step 6 To confirm the deletion, click **OK**. Otherwise, click **Cancel**.

Step 7 When the deletion confirmation message appears, click **OK** again.

You can view the deletion status of the policies in the **Application QoS Policies** page. If the status shows deletion failed, do the following:

- a) Click the failed state link under **Deployment Status** in the **Application QoS Policies** page.
- b) In the **Undeployment Status** window, click **Retry** to delete the policy.

Clone an Application Policy

If an existing application policy has most of the settings that you want in a new policy, you can save time by cloning the existing policy, changing it, and then deploying it to a different scope.

Before you begin

You must have created at least one policy.

-
- Step 1** Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.
 - Step 2** Use the **Filter** field to locate the policy that you want to clone.
 - Step 3** Click the radio button next to the policy that you want to clone.
 - Step 4** From the **Actions** drop-down list, choose **Clone**.
 - Step 5** Configure the application policy, as needed. For information about the application policy settings, see [Create an Application Policy, on page 602](#).
 - Step 6** Do one of the following tasks:
 - Save the policy as a draft by clicking **Save Draft**. For more information, see [Policy Drafts, on page 598](#).
 - Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

To deploy the policy now, click the **Run Now** radio button and click **Apply**.

To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see [Policy Scheduling, on page 599](#).
- Note** The site time zone setting is not supported for scheduling application policy deployments.

Restore an Application Policy

If you create or make changes to a policy and then decide that you want to start over, you can restore the original QoS configuration that was on the device before you configured it using Cisco DNA Center.

-
- Step 1** Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.
 - Step 2** Use the **Filter** field to locate the policy that you want to reset.
 - Step 3** Click the radio button next to the policy.
 - Step 4** From the **Actions** drop-down list, choose **Undeploy Policy**.
 - Step 5** In the **Undeploy Policy** window, click the **Restore devices to original configurations** radio button and click **Apply**.
 - Step 6** Click **OK** to confirm the change or **Cancel** to cancel it.

You can view the restoration status of the policies in the **Application QoS Policies** window. If the status shows restoration failed, do the following:

- a) Click the failed state link under **Deployment Status** in the **Application QoS Policies** window.
- b) In the **Undeployment Status** window, click **Retry** to restore the policy.

Reset the Default CVD Application Policy

The CVD configuration is the default configuration for applications. If you create or make changes to a policy and then decide that you want to start over, you can reset the applications to the CVD configuration. For more information about the CVD configuration, see [Application Policies Overview, on page 589](#).

-
- Step 1** Click the menu icon (**≡**) and choose **Policy > Application QoS > Application Policies**.
 - Step 2** Use the **Filter** field to locate the policy that you want to reset.
 - Step 3** Click the radio button next to the policy.
 - Step 4** From the **Actions** drop-down list, choose **Edit**.
 - Step 5** Click **Reset to Cisco Validated Design**.
 - Step 6** Click **OK** to confirm the change or **Cancel** to cancel it.
 - Step 7** Do one of the following tasks:
 - To save a draft of the policy, click **Save Draft**.
 - To deploy the policy, click **Deploy**.

Preview an Application Policy

Before you deploy a policy, you can generate the CLI that will be applied to a device and preview the configuration.

-
- Step 1** Click the menu icon (**≡**) and choose **Policy > Application QoS > Application Policies**.
 - Step 2** Create or edit a policy, as described in [Create an Application Policy, on page 602](#) or [Edit an Application Policy, on page 606](#).
 - Step 3** Before deploying the policy, click **Preview**.
A list of the devices in the scope appears.
 - Step 4** Click **Generate** next to the device that you are interested in.
Cisco DNA Center generates the CLIs for the policy.
 - Step 5** Click **View** to view the CLIs or copy them to the clipboard.
-

Precheck an Application Policy

Before you deploy an application policy, you can check whether the devices in the site scope are supported. The precheck process includes validating a device's model, line cards, and software image.

-
- Step 1** Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.
- Step 2** Create or edit a policy, as described in [Create an Application Policy, on page 602](#) or [Edit an Application Policy, on page 606](#).
- Step 3** Click **Pre-check**.
- Cisco DNA Center checks the devices and reports failures, if any, in the **Pre-Check Result** column. The **Errors** tab shows the devices that do not support this policy. The **Warnings** tab shows the restrictions or features that are not supported if you chose to deploy this policy in the device. You can still deploy the policy for the devices listed under **Warnings** tab. To resolve the failures, bring the devices into compliance with the specifications listed in the [Cisco DNA Center Compatibility Matrix](#).
-

Display Application Policy History

You can display the version history of an application policy. The version history includes the series number (iteration) of the policy and the date and time on which the version was saved.

-
- Step 1** Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.
- Step 2** Click the radio button next to the policy that interests you.
- Step 3** From the **Actions** drop-down list, choose **History**.
- Step 4** From the **Policy History** dialog box, you can do the following:
- To compare a version with the current version, click **Difference** next to the version that interests you.
 - To roll back to a previous version of the policy, click **Rollback** next to the version that you want to roll back to.
-

Roll Back to a Previous Policy Version

If you change a policy configuration, and then realize that it is incorrect, or that is not having the desired affect in your network, you can revert to a policy that is up to five versions back.

Before you begin

You must have created at least two versions of the policy to roll back to a previous policy version.

-
- Step 1** Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.
- Step 2** Click the radio button next to the policy that interests you.
- Step 3** From the **Actions** drop-down list, choose **Show History**.

Previous versions of the selected policy are listed in descending order, with the newest version (highest number) at the top of the list and the oldest version (lowest number) at the bottom.

Step 4 (Optional) To view the differences between the selected version and the latest version of a policy, click **Difference** in the **View** column.

Step 5 When you determine the policy version that you want to roll back to, click **Rollback** for that policy version.

Note If the selected site scope changed between policy versions, rollback is not done on the current (latest) selected site. Only the policy content is rolled back.

Step 6 Click **Ok** to confirm the rollback procedure.

The rolled back version becomes the newest version.

Manage Queuing Profiles

The following sections provide details about the various tasks that you can perform to manage queuing profiles.

Create a Queuing Profile

Cisco DNA Center provides a default CVD queuing profile (CVD_QUEUING_PROFILE). If this queuing profile does not meet your needs, you can create a custom queuing profile.

Step 1 Click the menu icon (☰) and choose **Policy > Application QoS > Queuing Profiles**.

Step 2 Click **Add Profile**.

Step 3 In the **Profile Name** field, enter a name for the profile.

Step 4 Configure the bandwidth for each traffic class by using the slider, clicking the plus (+) or minus (-) sign, or entering a specific number in the field.

The number indicates the percentage of the total interface bandwidth that will be dedicated to the selected application class. Because the total bandwidth equals 100, adding bandwidth to one application class subtracts bandwidth from another application class.

An open lock icon indicates that you can edit the bandwidth for the application class. A closed lock indicates that you cannot edit it.

If you make a mistake, you can return to the CVD settings by clicking **Reset to Cisco Validated Design**.

The graph in the middle helps you visualize the amount of bandwidth that you are setting for each application class.

Step 5 (For advanced users) To customize the DSCP code points that Cisco DNA Center uses for each of the traffic classes, from the **Show** drop-down list, choose **DSCP Values** and configure the value for each application class by entering a specific number in the field.

To customize the DSCP code points required within an SP cloud, configure an SP profile.

Step 6 Click **Save**.

Edit or Delete a Queuing Profile

- Step 1** Click the menu icon (☰) and choose **Policy > Application QoS > Queuing Profiles**.
- Step 2** From the **Queuing Profile** pane, click the radio button next to the queuing profile that you want to edit or delete.
- Step 3** Do one of the following tasks:
- To edit the profile, change the field values, except the profile name, and click **Save**. For information about the fields, see [Create a Queuing Profile, on page 612](#).
 - To delete the profile, click **Delete**.
- You cannot delete a queuing profile if it is referenced in an application policy.
-

Manage Application Policies for WAN Interfaces

The following sections provide details about the various tasks that you can perform to manage application profiles for WAN interfaces.

Customize Service Provider Profile SLA Attributes

If you do not want to use the default SLA attributes assigned to your SP profile by its class model, you can customize the SP profile SLA attributes to fit your requirements. For more information about the default SP profile SLA Attributes, see [Service Provider Profiles, on page 593](#).

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

- Step 1** Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.
- Step 2** Use the **Filter** field to locate the policy that you want to change.
- Step 3** Select the radio button next to the policy.
- Step 4** From the **Actions** drop-down list, choose **Edit**.
- Step 5** Click **SP Profiles** and select an SP profile.
- Step 6** You can modify the information in the following fields:
- **DSCP**: Differentiated Services Code Point (DSCP) value. Valid values are from 0 to 63.
 - Expedited Forwarding (EF)
 - Class Selector (CS): CS1, CS2, CS3, CS4, CS5, CS6
 - Assured Forwarding: AF11, AF21, AF41
 - Default Forwarding (DF)

For more information about these DSCP values, see [Marking, Queuing, and Dropping Treatments, on page 591](#).

- **SP Bandwidth %:** Percentage of bandwidth allocated to a specific class of service.
- **Queuing Bandwidth %:** Percentage of bandwidth allocated to each of the traffic classes. You can make one of the following changes:
 - To customize the queuing bandwidth, unlock the bandwidth settings by clicking the lock icon and adjust the bandwidth percentages.
 - To calculate the queuing bandwidth automatically from the SP bandwidth, lock the queuing bandwidth settings by clicking the lock icon and then clicking **OK** to confirm. By default, Cisco DNA Center automatically distributes the queuing bandwidth percentage such that the sum of the queuing bandwidth for all of the traffic classes in an SP class aligns with the SP bandwidth percentage of that class.

Step 7 Click **OK**.

Assign a Service Provider Profile to a WAN Interface

If you have already created an application policy and now want to assign SP profiles to WAN interfaces, you can edit the policy and perform this configuration, including setting the subline rate on the interface, if needed.

Before you begin

If you have not created a policy, you can create a policy and assign SP profiles to WAN interfaces at the same time. For more information, see [Create an Application Policy, on page 602](#).

- Step 1** Click the menu icon (☰) and choose **Policy > Application QoS > Application Policies**.
- Step 2** Use the **Filter** field to locate the policy that you want to edit.
- Step 3** Click the radio button next to the policy.
- Step 4** From the **Actions** drop-down list, choose **Edit**.
- Step 5** From the **Site Scope** pane, click the gear icon next to the site you are interested in.
- Step 6** Click **Configure** in the **SP Profile Settings** column for the device you are interested in.
- Step 7** In the **WAN Interface** column, from the **Select Interface** drop-down list, choose an interface.
- Step 8** In the **Role** column, from the **Select Role** drop-down list, choose a role according to the type of interface you are configuring:
- **Physical interface:** Choose **WAN**. This role is the only valid role for a physical interface.
 - **Tunnel interface:** Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.
- Note** Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.
- Step 9** In the **Service Provider Profile** column, click the **Select Profile** drop-down field and choose an SP profile.
- Step 10** If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.
- Step 11** To configure additional WAN interfaces, click + and repeat Step 7 through Step 10.
- Step 12** Click **Save**.

Step 13 Click < **Back to Site Scope**.

Step 14 Click **OK**.

Step 15 Click **Deploy**.

You are prompted to deploy your policy now or to schedule it for a later time.

Step 16 Do one of the following:

- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
- To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.



CHAPTER 26

Configure Traffic-Copy Policies

- [Traffic Copy Policies, on page 617](#)
- [Sources, Destinations, and Traffic Copy Destinations, on page 617](#)
- [Guidelines and Limitations of Traffic Copy Policy, on page 618](#)
- [Workflow to Configure a Traffic Copy Policy, on page 618](#)
- [Create a Traffic Copy Destination, on page 619](#)
- [Edit or Delete a Traffic Copy Destination, on page 619](#)
- [Create a Traffic Copy Contract, on page 619](#)
- [Edit or Delete a Traffic Copy Contract, on page 620](#)
- [Create a Traffic Copy Policy, on page 620](#)
- [Edit or Delete a Traffic Copy Policy, on page 620](#)

Traffic Copy Policies

Using Cisco DNA Center, you can set up an Encapsulated Remote Switched Port Analyzer (ERSPAN) configuration such that the IP traffic flow between two entities is copied to a specified destination for monitoring or troubleshooting.

To configure ERSPAN using Cisco DNA Center, create a traffic copy policy that defines the source and destination of the traffic flow that you want to copy. You can also define a traffic copy contract that specifies the device and interface where the copy of the traffic is sent.



Note Because traffic copy policies can contain either security groups or IP network groups, throughout this guide, we use the term *groups* to refer to both security groups and IP network groups, unless specified otherwise.

Sources, Destinations, and Traffic Copy Destinations

Cisco DNA Center simplifies the process of monitoring traffic. You do not have to know the physical network topology. You only have to define a source and destination of the traffic flow and the traffic copy destination where you want the copied traffic to go.

- **Source:** One or more network device interfaces through which the traffic that you want to monitor flows. The interface might connect to endpoint devices, specific users of these devices, or applications. A source

group comprises Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or port channel interfaces only.

- **Destination:** The IP subnet through which the traffic that you want to monitor flows. The IP subnet might connect to servers, remote peers, or applications.
- **Traffic Copy Destination:** Layer 2 or Layer 3 LAN interface on a device that receives, processes, and analyzes the ERSPAN data. The device is typically a packet capture or network analysis tool that receives a copy of the traffic flow for analysis.



Note At the destination, we recommend that you use a network analyzer, such as a Switch Probe device, or other Remote Monitoring (RMON) probe, to perform traffic analysis.

The interface type can be Ethernet, Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interfaces only. When configured as a destination, the interface can be used to receive only the copied traffic. The interface can no longer receive any other type of traffic and cannot forward any traffic except that required by the traffic copy feature. You can configure trunk interfaces as destinations. This configuration allows the interfaces to transmit encapsulated traffic.



Note There can be only one traffic copy destination per traffic copy contract.

Guidelines and Limitations of Traffic Copy Policy

The traffic copy policy feature has the following limitations:

- You can create up to 8 traffic copy policies, 16 copy contracts, and 16 copy destinations.
- The same interface cannot be used by more than one traffic copy destination.
- Cisco DNA Center does not show a status message to indicate that a traffic copy policy has been changed and is no longer consistent with the one that is deployed in the network. However, if you know that a traffic copy policy has changed since it was deployed, you can redeploy the policy.
- You cannot configure a management interface as a source group or traffic copy destination.

Workflow to Configure a Traffic Copy Policy

Before you begin

- To be monitored, a source security group that is used in a traffic copy policy needs to be statically mapped to the switches and their interfaces.
- A traffic copy policy destination group needs to be configured as an IP network group. For more information, see [Create an IP Network Group, on page 585](#).

Step 1 Create a traffic copy destination.

This is the interface on the device where the traffic flow will be copied for further analysis. For information, see [Create a Traffic Copy Destination, on page 619](#).

Step 2 Create a traffic copy contract.

The contract defines the copy destination. For information, see [Create a Traffic Copy Contract, on page 619](#).

Step 3 Create a traffic copy policy.

The policy defines the source and destination of the traffic flow and the traffic copy contract that specifies the destination where the copied traffic is sent. For information, see [Create a Traffic Copy Policy, on page 620](#).

Create a Traffic Copy Destination

Step 1 Click the menu icon (☰) and choose **Policy > Traffic Copy > Traffic Copy Destination**.

Step 2 Enter a name and description for the traffic copy destination.

Step 3 Select the device and one or more ports.

Step 4 Click **Save**.

Edit or Delete a Traffic Copy Destination

Step 1 Click the menu icon (☰) and choose **Policy > Traffic Copy > Traffic Copy Destination**.

Step 2 Check the check box next to the destination that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
 - To delete the destination, click **Delete**.
-

Create a Traffic Copy Contract

Step 1 Click the menu icon (☰) and choose **Policy > Traffic Copy > Traffic Copy Contract**.

Step 2 Click **Add**.

Step 3 In the dialog box, enter a name and description for the contract.

Step 4 From the **Copy Destination** drop-down list, choose a copy destination.

Note You can have only one destination per traffic copy contract.

If no copy destinations are available for you to choose, you can create one. For more information, see [Create a Traffic Copy Destination, on page 619](#).

Step 5 Click **Save**.

Edit or Delete a Traffic Copy Contract

Step 1 Click the menu icon () and choose **Policy > Traffic Copy > Traffic Copy Contract**.

Step 2 Check the check box next to the contract that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
 - To delete the contract, click **Delete**.
-

Create a Traffic Copy Policy

Step 1 Click the menu icon () and choose **Policy > Traffic Copy > Traffic Copy Policies**.

Step 2 Click **Add Policy**.

Step 3 In the **Policy Name** field, enter a name.

Step 4 In the **Description** field, enter a word or a phrase that identifies the policy.

Step 5 In the **Contract** field, click **Add Contract**.

Step 6 Click the radio button next to the contract that you want to use and then click **Save**.

Step 7 Drag and drop groups from the **Available Groups** area to the **Source** area.

Step 8 Drag and drop groups from the **Available Groups** area to the **Destination** area.

Step 9 Click **Save**.

Edit or Delete a Traffic Copy Policy

Step 1 Click the menu icon () and choose **Policy > Traffic Copy > Traffic Copy Policies**.

Step 2 Check the check box next to the policy that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
 - To delete the policy, click **Delete**.
-



PART **VII**

Monitor and Troubleshoot Your Network

- [Cisco AI Endpoint Analytics, on page 625](#)
- [Troubleshoot Network Devices Using Network Reasoner, on page 677](#)
- [Identify Network Security Advisories, on page 691](#)



CHAPTER 27

Cisco AI Endpoint Analytics

- [Cisco AI Endpoint Analytics Overview, on page 625](#)
- [Key Features of Cisco AI Endpoint Analytics, on page 626](#)
- [FIPS Compliance, on page 627](#)
- [Set Up Cisco AI Endpoint Analytics in Cisco DNA Center, on page 628](#)
- [Cisco AI Endpoint Analytics Overview Window, on page 632](#)
- [Endpoint Inventory, on page 641](#)
- [Trust Score, on page 645](#)
- [Profiling Rules, on page 661](#)
- [Cisco AI Rules for Smart Grouping, on page 667](#)
- [Hierarchy, on page 673](#)

Cisco AI Endpoint Analytics Overview

Visibility is the first step towards securing an endpoint. Cisco AI Endpoint Analytics is an endpoint visibility solution that helps you identify and profile endpoints and Internet of Things (IoT) devices. The Cisco AI Endpoint Analytics engine enables you to assign labels to endpoints, using the telemetry information received from the network from various sources.

The profiling labels that are available in Cisco AI Endpoint Analytics are endpoint type, hardware model, manufacturer, and operating system type. This is called multifactor classification.

Cisco AI Endpoint Analytics provides nuanced visibility and enforcement in your network with features like Trust Scores that allow you to identify and act upon potentially risky endpoints and devices. You can also manage potential risks by applying ANC policies through Cisco ISE, from the Cisco AI Endpoint Analytics GUI. You can monitor and work around the issue of random and changing MAC addresses from endpoints in Cisco AI Endpoint Analytics and accurately identify endpoints through a unique attribute called the DUID instead of MAC addresses.

Cisco AI Endpoint Analytics helps you gather endpoint telemetry from different sources. The primary source is the Network-Based Application Recognition (NBAR) mechanism. The NBAR mechanism is embedded in Cisco Catalyst 9000 Series switches (access devices) and performs deep packet inspection (DPI). Cisco AI Endpoint Analytics can also receive telemetry from Cisco DNA Traffic Telemetry Appliances.

You can gather endpoint context information from various sources such as Cisco ISE, self-registration portals, and configuration management database (CMDB) software such as ServiceNow.

Cisco AI Endpoint Analytics allows data inflow from a wide range of network devices, expanding your ability to easily identify and profile endpoints with greater accuracy, and act upon any anomalies. You can aggregate

varied endpoint information and use the data to profile endpoints in Cisco AI Endpoint Analytics. After endpoints are profiled, AI and machine learning algorithms can also be used to reduce the number of unknown endpoints by intuitively leveraging different methods.

Key Features of Cisco AI Endpoint Analytics

- **Cisco AI Endpoint Analytics dashboard**

The Cisco AI Endpoint Analytics dashboard gives you a comprehensive view of the endpoints that are connected to your network. You can view the number of known, unknown, profiled, and unprofiled endpoints, endpoints with low Trust Scores, and endpoints that use random MAC addresses. The AI Proposals dashlet displays intelligent profiling suggestions to enhance endpoint profiling and management.

- **Trust Scores to flag potentially risky endpoints**

Cisco AI Endpoint Analytics assigns Trust Scores to endpoints to allow you to easily monitor and act on potentially risky endpoints in your network. Behavioral anomalies are monitored and tracked, and a Trust Score is assigned based on the number and frequency of the anomalies tracked. See [Trust Scores for Endpoints, on page 646](#).

- **Detect endpoints that use random MAC addresses**

Cisco AI Endpoint Analytics enables you to handle the issue of random and changing MAC addresses by receiving from Cisco ISE a unique endpoint identifier called the DUID (also known as GUID in Cisco ISE). Cisco AI Endpoint Analytics then uses the DUID as the identifier for an endpoint, instead of its MAC address.

- **Reduce net unknowns with machine learning capabilities**

Cisco AI Endpoint Analytics provides profiling suggestions based on learnings from endpoint groupings. You can use these suggestions to reduce the number of unknown or unprofiled endpoints in your network.

- **Manage endpoints with system and custom profiling rules**

Use Cisco-provided system rules and custom rules of your design to reliably profile and manage the endpoints connected to your network.

- **Registration of endpoints through Cisco AI Endpoint Analytics**

You can onboard and profile endpoints using Cisco AI Endpoint Analytics. The endpoint attribute data that is collected through this registration process is used to profile the endpoints.

- **Registration of endpoints using external sources**

You can connect some external sources of endpoint data, such as Configuration Management Databases (CMDB), to Cisco AI Endpoint Analytics. This allows you to easily register, manage, and profile endpoints in your network.

- **Purge endpoints after a defined period of inactivity**

Define an Endpoint Purge Policy to remove from your network the endpoints that have been inactive for a defined time. You can define the period of inactivity after which an endpoint must be removed. You can also customize a purge policy to act on a particular set of endpoints based on a profiling attribute.

FIPS Compliance

Cisco DNA Center supports the United States' Federal Information Processing Standards (FIPS). FIPS is an optional mode that can be enabled when installing the Cisco DNA Center image. By default, FIPS mode is disabled.

When FIPS mode is enabled in Cisco DNA Center, the following functions in the Cisco DNA Center GUI are *unavailable*:

- The **Enable AI Network Analytics** dashlet in the **Optional Configurations** section in **AI Endpoint Analytics Setup**.
- The **AI Proposals** dashlet in **Policy > AI Endpoint Analytics > Overview**.
- The **Profile Rule Settings** tab in **Policy > AI Endpoint Analytics > Overview > Configuration**.
- The **AI Spoofing Detection** section in **Policy > AI Endpoint Analytics > Overview > Configuration > Trust Analytics**.
- The **AI Spoofing Detection** section in **Endpoint Anomaly Detection** under **Trust Score** details for a particular endpoint in **Policy > AI Endpoint Analytics > Endpoint Inventory**.
- The **AI Spoofing Detection** column in **Policy > AI Endpoint Analytics > Endpoint inventory > Focus as Trust Score**.



Note Talos IP Reputation is not supported when FIPS is enabled.

Set Up Cisco AI Endpoint Analytics in Cisco DNA Center

Set Up Cisco AI Endpoint Analytics

Software Updates

Download and install the following software packages:

- Cisco AI Endpoint Analytics
- AI Network Analytics (Optional)
- Application Visibility Service

Join and Configure Data Sources

Join and configure the following data sources:

- Cisco Identity Services Engine
- Cisco Catalyst 9000 Series Access Devices for wired endpoints visibility
- (Optional) Cisco DNA Traffic Telemetry Appliances (DN-APL-TTA-M) for wired and wireless endpoints visibility, and for third-party network devices visibility
- (Optional) Cisco Catalyst 9800 Series Wireless Controllers for wireless endpoints visibility
- (Optional) CMDB

Install Software Updates

Install software updates in Cisco DNA Center to use Cisco AI Endpoint Analytics, as described in the following procedure.

-
- Step 1** Log in to Cisco DNA Center.
- Step 2** Click the menu icon (☰) and choose **System > Software Management**.
- Step 3** In the **Updates** tab, check if **Cisco AI Endpoint Analytics**, **AI Network Analytics**, and **Application Visibility Service** are listed in the **Application Updates** section. If these application updates are visible, click **Install All**.
- Install the **Cisco AI Endpoint Analytics** update to access the endpoint profiling solution in your Cisco DNA Center.
 - Install the **AI Network Analytics** update to use machine learning and AI capabilities to receive intelligent profiling suggestions.
 - Install the **Application Visibility Service** update to use NBAR and Controller-Based Application Recognition (CBAR) techniques to inform endpoint profiling.
- Step 4** If these updates aren't listed in the **Updates** tab, click the **Installed Apps** tab to check if the updates are already installed and are available for use. The **Currently Installed Applications** tab also confirms if the software installation succeeded.
-

Connect and Enable Data Sources

The data sources that Cisco AI Endpoint Analytics uses may already be connected to your Cisco DNA Center. If the data sources are connected, see the following instructions to ensure that the data sources are available for use by Cisco AI Endpoint Analytics.

You must add Cisco ISE or Catalyst 9000 Series access devices to Cisco DNA Center for Cisco AI Endpoint Analytics to provide results.

Step 1

Connect Cisco ISE to Cisco DNA Center:

See the "Integrate Cisco ISE with Cisco DNA Center" section in "Complete First-Time Setup" in the [Cisco DNA Center Appliance Installation Guide](#).

The following Cisco ISE releases support Cisco AI Endpoint Analytics:

- 2.4 Patch 11 and later
- 2.6 Patch 5 and later
- 2.7 Patch 1 and later
- 3.0 and later

For Cisco ISE release 3.1 and later, in your Cisco ISE administration portal:

- a) Choose **Work Centers > Profiler > Settings**.
- b) In the **Endpoint Analytics Settings** area, check the following check boxes:
 - **Publish Endpoint Attributes to AI Endpoint Analytics**
 - **Consume Endpoint Profiles from AI Endpoint Analytics**

After Cisco ISE authenticates endpoints through 802.1X or MAB authentication methods, the endpoint attributes collected are made available to Cisco AI Endpoint Analytics. Cisco ISE also shares telemetry data with Cisco AI Endpoint Analytics.

For Cisco ISE releases 2.4, 2.6, and 3.0, in your Cisco ISE administration portal:

- a) Choose **Work Centers > Profiler > Settings**.
- b) Choose the **Enable Probe Data Publisher** option.
- c) Click **Save**.

Step 2

Connect Cisco 9000 Series access devices to Cisco DNA Center for wired endpoints visibility.

See "Discover Your Network" in the [Cisco DNA Center User Guide](#).

To enable Cisco AI Endpoint Analytics features, upgrade your Cisco 9000 Series access devices to Cisco IOS-XE Release 17.6 or later.

To enable CBAR for the required access devices:

- a) In the Cisco DNA Center GUI, click the menu icon (☰) and choose **Provision > Services > Application Visibility**.
- b) Select the Cisco Catalyst 9000 access device that you need data from. Check the check box next to the device name in the **Site Devices** section.
- c) Click **Enable CBAR**.
- d) Click **Yes** in the subsequent confirmation window.

- e) In the **Enable CBAR** slide-in pane, check the check box next to the supported SSID type.
- f) Click **Enable**.

Step 3 (Optional) Connect Cisco Catalyst 9800 Series Wireless Controllers to Cisco DNA Center for wireless endpoints visibility.

The following Cisco Catalyst 9800 Series Wireless Controller models are supported by Cisco AI Endpoint Analytics:

- 9800-CL
- 9800-40
- 9800-80
- 9800-L

Cisco DNA Center Release 2.3.2 and later supports FlexConnect in Cisco Catalyst 9800 Series Wireless Controllers with Cisco IOS XE Release 17.7.1 and later.

To configure and provision a Cisco Catalyst 9800 Series Wireless Controller in Cisco DNA Center, see [Cisco Catalyst 9800 Series Wireless Controller Overview, on page 403](#).

Step 4 (Optional) Connect Cisco Catalyst IE9300 Rugged Series switches to Cisco DNA Center.

The Cisco Catalyst IE9300 Rugged Series switches are supported by Cisco AI Endpoint Analytics.

See “Discover Your Network” in the [Cisco DNA Center User Guide](#).

Step 5 (Optional) Connect Cisco DNA Traffic Telemetry Appliances to Cisco DNA Center for wired and wireless endpoints visibility, and for third-party network device visibility.

Cisco DNA Traffic Telemetry Appliances (DN-APL-TTA-M) generate telemetry from mirrored network traffic for endpoint analytics. This appliance enables Network-Based Application Recognition-based (NBAR-based) protocol inspection and endpoint attribute extraction.

To receive endpoint attributes collected through the telemetry appliance in Cisco AI Endpoint Analytics, you must integrate Cisco ISE with Cisco DNA Center.

See [Cisco DNA Traffic Telemetry Appliances](#) for information on installing the appliances, connectivity configurations, and managing the appliances in Cisco DNA Center.

Enable CBAR on Switched Port Analyzer (SPAN)-receiving ports of access switches connected to Cisco DNA Traffic Telemetry Appliances with the following command:

```
ip nbar protocol-discovery
```

Not all endpoints that are connected to the telemetry appliances are visible in Cisco AI Endpoint Analytics. Only endpoints that are also connected to Network Access Devices (NADs) that are managed in Cisco DNA Assurance are visible in Cisco AI Endpoint Analytics.

Step 6 (Optional) Enable ServiceNow in Cisco DNA Center.

- a) After connecting ServiceNow to Cisco DNA Center, click the menu icon (≡) and choose **Platform > Manage > Bundles**.
- b) If the **Status** of the bundle **Endpoint Attribute Retrieval with ITSM (ServiceNow)** is **New**, click **Enable** for the bundle.

Step 7 (Optional) Enable Cisco AI Analytics in Cisco DNA Center.

To receive suggestions about AI-based endpoint groupings, automated custom profiling rules, and endpoint labels, and to detect potentially spoofed devices in your network, you must enable the required settings in the **Cisco AI Analytics** window.

You must install the AI Network Analytics software to receive these AI-based suggestions.

- a) Click the menu icon (☰) and choose **System > Settings > External Services > Cisco AI Analytics**.
- b) Click the toggle button for each of the following services that you want to enable:
 - **AI Endpoint Analytics:** AI Network Analytics leverages machine learning to drive intelligence in the network and enables you to effectively improve network performance and accelerate issue resolution. AI Network Analytics significantly reduces noise and false positives by analyzing network behavior and adapting to your network environment.
 - **Endpoint Smart Grouping:** Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in your network by providing AI-based endpoint groupings, automated custom profiling rules, and crowdsourced endpoint labels.
 - **AI Spoofing Detection:** AI Spoofing Detection identifies spoofed endpoints based on pretrained behavioral models. Enabling the **Enable AI Spoofing Detection** toggle button allows Cisco DNA Center to detect spoofed endpoints using these behavioral models and the flow information provided by the network devices. Several behavioral models are built and centrally trained using the collected flow information gathered from participating customers.
 - Spoofing detection is performed in the cloud and anonymized data export to the cloud from Cisco DNA Center is mandatory. Cisco DNA Center then polls the cloud for spoofing detections.
 - Having an uninterrupted internet connection is required for this feature to work.
 - While upgrading to the latest release, if data export was disabled in the previous version, a warning stating that data export is disabled is displayed to the user upon upgrade. Spoofing Detection must be re-enabled by the user.

Endpoint Telemetry Sources

Cisco AI Endpoint Analytics receives telemetry data in the following ways.

- **Deep Packet Inspection**

Deep packet inspection is an advanced method of packet analysis that is carried out by Cisco Catalyst 9000 Series access devices. These access devices run NBAR, which inspects application traffic and performs protocol analysis to discover, identify, and profile endpoints with high fidelity.

Deep packet inspection profiling is based on various attributes that are collected from endpoint traffic to the network. These attributes are collected across multiple protocols, from packet header layers 4 to 7.

- **Configuration Management Database Connection**

Cisco AI Endpoint Analytics receives endpoint data from your Configuration Management Database Connection (CMDB) for greater accuracy in endpoint profiling. The connection with ServiceNow enables you to receive information from the CMDB to Cisco AI Endpoint Analytics.

- **Machine Learning Capabilities**

Data collected for profiling is anonymized and sent to a Cisco cloud location that serves as a device data lake. Here, machine learning algorithms analyze the data available to create profiling rules that you can evaluate and apply, as needed. Smart profiling rules are suggested through Cisco AI Endpoint Analytics to help make endpoint profiling and management simpler and more efficient for you. Existing rules too are evaluated and improvement suggestions provided based on this continuous learning.

Cisco AI Endpoint Analytics Overview Window

Click the menu icon (☰) and choose **Policy > AI Endpoint Analytics**.

The **Overview** window displays the following dashlets:

• Total Endpoints

This dashlet displays the total number of endpoints in your network in two groups, **Fully Profiled** and **Partially Profiled**. Cisco AI Endpoint Analytics profiles endpoints based on four factors, Endpoint Type, OS Type, Hardware Model, and Hardware Manufacturer. If one or more of these factors are missing for an endpoint, it is profiled in the **Partially Profiled** group.

Click **Partially Profiled Labels** to view the number of endpoints in your network with missing profiles, categorized by profile label type. To check the endpoints with a specific missing profile label, click the number next to the profile label. The **Endpoint Inventory** tab is displayed with the corresponding list of endpoints.

• AI Proposals

Cisco AI Endpoint Analytics uses smart grouping algorithms to group unknown endpoints in your network that have similar profiling data. If you have enabled AI Endpoint Analytics, you will receive the following types of rule proposals. These rule proposals are based on learnings from endpoint clusters:

- New rules for profiling endpoints that may be similar.
- Modification proposals for previously accepted rules.
- Review of profiling rules that are no longer needed.

For more details, see [Cisco AI Rules for Smart Grouping, on page 667](#).

• Trust Scores

The Trust Scores dashlet provides an overall view of the Trust Scores assigned to the endpoints in your network. See [Trust Scores for Endpoints, on page 646](#).

• Configuration

Click the **Configuration** link in the top-right corner of the Overview area to access the following configurations:

- **Profile Rule Settings:** Schedule automatic updates for system profile rules. See [Automatic System Rule Updates for Endpoint Profiling, on page 663](#).
- **ISE Integration:** See [Publish Authorization Attributes to Cisco ISE, on page 636](#).
- **Trust Analytics:** Click the toggle buttons to enable or disable Trust Score sources. You cannot disable the **Authentication Method** source. If an active Cisco ISE integration is configured, the authentication method used by the endpoint and its posture status will inform the Trust Score of an

endpoint. You can enable or disable other sources of Trust Score data such as **AI Spoofing Detection**, **Endpoint Attribute Conflict**, **NAT Mode Detection**, **Concurrent MAC Addresses**, and **Security Sensor**.

See [Trust Scores for Endpoints](#), on page 646.

- **Endpoint Purge Policy:** See [Endpoint Purge Policies](#), on page 639.
- **Endpoint Subnet Inspection:** See [Configure Endpoint Subnet Inspection](#), on page 640.

- **Endpoint MAC Randomization**

The Endpoint MAC Randomization displays the number of static MAC addresses and random and changing MAC addresses in the network. See [Trust Scores for Endpoints with Random and Changing MAC Addresses](#), on page 652.

Integrate Cisco AI Endpoint Analytics with Talos Intelligence

Talos Intelligence is a comprehensive threat-detection network. Talos Intelligence is composed of threat detection analysts and real-time automated detection systems that span web requests, emails, malware samples, open-source data sets, endpoint intelligence, and network intrusions. Integrate Cisco AI Endpoint Analytics with Talos to flag network connections reaching out to untrusted IP addresses, quarantining them, and protecting your network from the most common cyber threats.

Cisco DNA Cloud communicates with the Talos Intelligence Cloud Service to obtain the updated IP Reputation data every 30 minutes. This update in the IP Reputation data is pushed to all the registered Cisco DNA Center devices.

To set up Talos Intelligence on your Cisco DNA Center device, complete the following steps.

Before you begin

The prerequisites for integrating Cisco AI Endpoint Analytics with Talos Intelligence are:

- Cisco DNA Center must be registered with Cisco DNA Cloud.

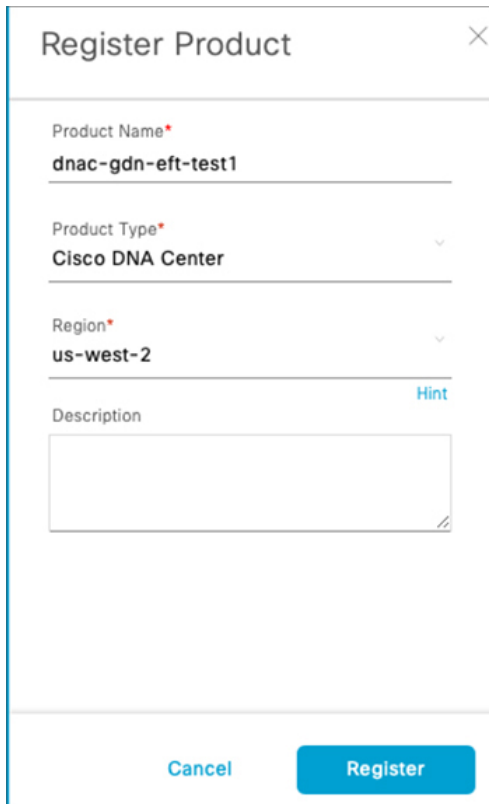


Note When a user isn't registered with Cisco DNA Cloud, a warning is displayed next to the toggle button under the **Talos IP Reputation** setting in the Cisco DNA Center GUI.

- The account must be subscribed to the Talos offer on Cisco DNA Cloud.
- For the Talos IP Reputation feature to work smoothly, enable application telemetry and choose Cisco DNA Center as the NetFlow collector.

-
- Step 1** In the Cisco DNA Center GUI, click the menu icon (☰) and choose **System > Settings > External Services > Cloud Authentication**.
- Step 2** Click the **dna.cisco.com** link and create a Cisco DNA Cloud account. On Cisco DNA Cloud, subscribe to the Talos offer and select the appropriate Cisco DNA Center region.

Figure 27: Subscribe to Talos Offer



The image shows a 'Register Product' dialog box with the following fields and values:

- Product Name***: dnac-gdn-eft-test1
- Product Type***: Cisco DNA Center
- Region***: us-west-2
- Description**: (Empty text area with a 'Hint' link to the right)

At the bottom of the dialog are two buttons: 'Cancel' and 'Register'.

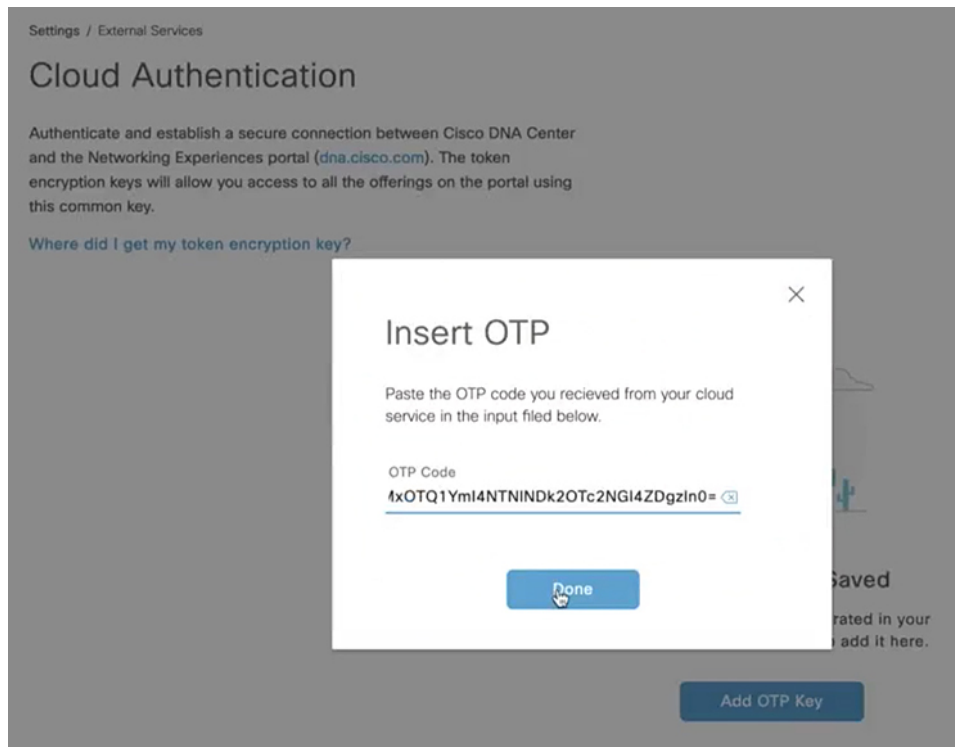
Step 3 Under **On-prem Connections**, register your Cisco DNA Center device. A one-time password (OTP) is sent to your device. This OTP is valid for 30 minutes.

Figure 28: OTP That Is Sent to Your Device



- Step 4** On the Cisco DNA Center home page, register your Cisco DNA Center device to Cisco DNA Cloud using the OTP for cloud authentication (**System-Settings > Cloud Authentication**).

Figure 29: Register Cisco DNA Center to Cisco DNA Cloud



Note After registering your Cisco DNA Center device to Cisco DNA Cloud, wait for 3 minutes before proceeding to Step 4.

- Step 5** On the Cisco DNA Center **AI Endpoint Analytics** window (**AI Endpoint Analytics > Configurations > Trust Analytics**), click the **Talos IP Reputation** toggle button to enable it. You can enable **Talos IP Reputation** from either the **Trust Score** window or the **Cisco DNA Center System Settings** window. After **Talos IP Reputation** is enabled, Cisco DNA Center receives the updated IP Reputation data whenever it's available. If an endpoint in the network tries to access an untrusted IP address, it's flagged, and a warning message stating `Detected` is displayed for Talos IP Reputation in the Trust Score view for an endpoint. This warning reduces the overall Trust Score of the endpoint. The Talos IP Reputation feature stores information about the untrusted IP addresses accessed and the number of access attempts made by an endpoint. This information is useful when deciding about increasing the security of the network.

The **Talos Reputation** window (**Cisco DNA Center System Settings > Talos IP Reputation**) displays the latest versions of various files received from Talos. The time when these files were received is also displayed. IPv4 and IPv6 files are Talos IP reputation data files, and are typically updated once a day. However, the *Threat Level* file is metadata and changes in this file are rare.

Publish Authorization Attributes to Cisco ISE

Publish Cisco AI Endpoint Analytics profile data to Cisco ISE to authorize endpoint access to the network and for endpoint control. The attribute information that is shared by Cisco AI Endpoint Analytics is then easily accessible to a Cisco ISE administrator through the AI Endpoint Analytics dictionary. A Cisco ISE administrator can easily create authorization policies in Cisco ISE. The following attributes are shared with Cisco ISE:

1. The overall trust score and the score for each anomaly that is recorded.
2. CMDB attributes.
3. Multifactor profiling attributes: Hardware Manufacturer, Hardware Model, Operating System, and Endpoint Type.

If your Cisco DNA Center has an active integration with Cisco ISE Release 3.1 and later releases, and you want to publish authorization attributes to Cisco ISE, carry out the following tasks.

Step 1

To enable attribute sharing in Cisco DNA Center, do the following:

- a) In the Cisco AI Endpoint Analytics **Overview** window, click **Configurations**.
- b) Click **ISE Integration** from the left panel.
- c) Click the **Enable Profile Publishing to ISE** toggle button to enable the feature.
- d) Check the **Asset Topic Based Integration** or **Enhanced Authorization Integration** check boxes, or both, depending on which type of topic you want to use to publish attribute information to Cisco ISE.
- e) Click **Save**.

Step 2

To enable pxGrid subscription in Cisco ISE, do the following:

- a) In the Cisco ISE GUI, click the menu icon and choose **Work Center > Profiler > Settings**.
- b) If you are connected to Cisco ISE Release 3.1, in the **Endpoint Analytics Settings** area, check the following check boxes:
 - **Publish Endpoint Attributes to AI Endpoint Analytics**
 - **Consume Endpoint Profiles from AI Endpoint Analytics**

What to do next

To verify the subscription, from the Cisco ISE main menu, choose **Administration > pxGrid Services > Diagnostics > WebSocket > Clients**. The newly created subscription containing `"com.cisco.ea.data.ise-<Cisco ISE node>"` is displayed in the **Subscription** column of the PSN nodes.

In the Cisco ISE **Policy > Policy Sets** window, a new dictionary that is named **Endpoint-Analytics** is visible in the Conditions Studio.

In the Cisco ISE **Context Visibility > Endpoints** window, click **MAC Address** for endpoint details. The attributes area of the details displays attributes that contain "EA-" prefixes for the attributes that are received from Cisco AI Endpoint Analytics.

Trust Analytics

The **Trust Analytics** window displays the various trust score sources, enables you to reset alerts raised on these sources manually or automatically after a period of inactivity, and sets the impact level for each trust score source to accurately measure the overall trust score of an endpoint.

Trust Score assesses the trustworthiness of a given endpoint on the network to help achieve zero trust outcomes. Values range from 1 (low trust) to 10 (high trust) and are calculated using several sources:

- **Endpoint Context:** This category of sources provides information about the reliability of an endpoint, by knowing the authentication method used by the endpoint and posture status of the endpoint.
- **Threat and vulnerability Context:** This category of sources provides information about how vulnerable an endpoint is based on the various types of threats associated with an endpoint.
- **Network Context:** This category of sources provides information about how an endpoint is accessing the network.

Trust Score Impact allows you to control the trust score of an endpoint when an anomaly is raised. The following impact levels are available:

- **Low:** When you know that an anomaly is of low importance in your network, you can set its impact level to **Low** so that it has a low impact on the trust score. After setting this impact level, when such an anomaly is detected again, the trust score for the endpoint on which the anomaly is detected sluggishly reduces to 1 (Increases system-generated impact level by 50% of total trust score).
- **Critical:** When you know that an anomaly is of high importance in your network, you can set its impact level to **Critical** so that it has a very high impact on the trust score. After setting this impact level, when such an anomaly is detected again, the trust score for the endpoint on which the anomaly is detected quickly reduces to 1 (Reduces system-generated impact level by 50% of total trust score).
- **No Impact:** An anomaly is detected, but does not impact the overall trust score. You can use this option to test out the anomalies and view them without changing the overall trust score.
- **System Default:** Default system-generated trust score.

To know how to customize impact levels for the sources, see [Customize Impact Level](#).

Alerts appear when there is a deviation caused by anomalies or vulnerabilities, or when a weakness is identified in endpoint connections or interfaces. The alerts can be reset manually after addressing them. You can also manually reset the alerts you don't want to address. Alternatively, you can set a reset timer to reset the alerts automatically. After a period of inactivity, this alert is not detected on endpoints.

To know how to reset alerts for the sources, see [Configure Reset Alert](#).

Customize Impact Level

You can now customize the trust score of an endpoint by setting an impact level that you perceive for an endpoint. Based on the impact level that you set for a source, the overall trust score is recalculated for the endpoints. This gives you the authority to decide the trust level of an anomaly irrespective of the system-generated trust score for that anomaly.



Note For authentication method EAT-TLS and posture non-compliant endpoints, even if you change the impact level, the trust level remains the same. The trust level is only changed in the case of MAB authentication.



Note The high trust score that is earned because of the authentication method used, is not lowered even when the impact level for the authentication method is changed. If the impact level for the authentication method is increased, the endpoints continue to retain their current trust score unless a new session for that endpoint is received.

-
- Step 1** Click the menu icon (☰) and choose **Policy > AI Endpoint Analytics > Overview > Manage Sources**. The **Trust Analytics** window opens.
- Step 2** Click **Customize Impact Level**.
- Step 3** Click **Let's Do It**.
The **Customize Trust Score Sources** workflow begins. You can exit the workflow at any point in time by clicking the **Exit** option at the bottom of the workflow window.
- Step 4** Check the checkboxes next to the sources for which you want to change the impact level.
- Step 5** From the **More Actions** drop-down list, choose the **New Impact Level**.
- Step 6** Click **Next**.
In the next window, a comparative study of the previous and new trust score is provided that shows the trust score customization impact on individual endpoints. This pie chart includes all the endpoints in the network irrespective of whether or not they were impacted by the change in the impact level of the sources. The **Endpoints (After)** table below displays the new trust score for each endpoint that was impacted as a result of the change in the impact level configuration.
- Step 7** Click **Next**.
A summary stating the new impact level of each source is displayed. Click **Edit** to go back in the workflow to edit the impact level of the trust scores in case you are not satisfied with the result.
- Step 8** Click **Next**.

The endpoints' trust scores are updated accordingly and is also sent to Cisco ISE. This may result in a change of authorization for such endpoints if Cisco ISE is using trust score based authorization policies.

What to do next

Check the new trust score for the endpoints in **Policy > AI Endpoint Analytics > Trust Score**.

Configure Reset Alert

You can reset an alert manually or automatically after a period of inactivity. By default, the reset action is set to **Manual** for all supported sources. You can configure to reset an alert using the global configuration workflow as described here.

-
- Step 1** Click the menu icon (☰) and choose **Policy > AI Endpoint Analytics > Manage Sources**. The **Trust Analytics** window opens.
- Step 2** Click **Alert Configuration**.
- Step 3** In the **Choose Reset Alert Type** window, click **Let's Do It**.

You can exit the workflow at any point in time by clicking the **Exit** option at the bottom of the workflow window.

- Step 4** From the **Reset Alert Type** drop-down list, choose **Manual** or **Customize reset timer after alert inactivity**.
- Step 5** If you choose **Customize reset timer after alert inactivity**, enter the number of days (0 to 365 days) or hours (0 to 24 hours), after which you want to reset the alert, in case of inactivity.
- You can choose to remove or retain the ANC Policy. If the endpoint has a trust value from more than one trust score source, the ANC policy will not be removed even if the **Remove ANC Policy** checkbox is checked.
- Step 6** Click **Next**.
- Step 7** Check the check boxes next to all the sources for which you want to apply the setting that you chose in Step 4.
- Step 8** Click **Apply**.

You can also configure to reset an alert locally from the **Trust Analytics** window. Choose the source for which you want to configure the reset alert. In the slide-in window on the right, choose the appropriate setting and click **Save**. Note that the reset alert configuration option is not available for all sources. When the alerts are reset, the same information is propagated back to Cisco ISE.

The alerts are checked every 30 minutes for an update. And if, during any of the checks, the time period configured in the reset alert configuration has lapsed, the trust score is reset for that anomaly. The status of the reset alert will be displayed in the Audit log.

Endpoint Purge Policies

Define an Endpoint Purge Policy to remove from your network the endpoints that have been inactive for a defined time. You can define the period of inactivity after which an endpoint must be removed. You can also customize a purge policy to act on a particular set of endpoints based on a profiling attribute. Purge policies are executed at 2 A.M. (server time) every day, and the endpoints that meet the defined purge requirements are removed from your network.

Registered endpoints and static endpoints that are imported into Cisco AI Endpoint Analytics are not affected by endpoint purge policies.

The Backup and Restore operation in your Cisco DNA Center and the endpoint purge activity cannot run simultaneously. If a Backup and Restore operation is in progress at 2 A.M., the purge activity is not initiated. If a Backup and Restore operation starts while an endpoint activity is in progress, the endpoint purge stops running, and the purge activity is left incomplete. The remaining endpoints are not acted on until the next purge is executed at 2 A.M. (server time) the next day.

To view, edit, or add endpoint purge policies, click the menu icon (☰) and choose **Policy > AI Endpoint Analytics > Configurations > Endpoint Purge Policy**. The following policies are available by default:

- **Default**
- **Random MAC Default**

You cannot edit these default policies. You can only enable or disable them.

You can use the **Purge Now** option to immediately run the purge policy instead of waiting until 2 AM. There are two ways to use the **Purge Now** option:

- Select the purge policies that you want to run now and choose **Purge Now** from the **More Actions** drop-down list.

- Click the icon under the **Actions** column for the purge policy that you want to run now and choose **Purge Now**.

Create a Purge Policy

- Step 1** Click the menu icon (☰) and choose **Policy > AI Endpoint Analytics > Configurations > Endpoint Purge Policy**.
- Step 2** Click **Add Endpoint Purge Policy**.
- Step 3** In the **Add Endpoint Purge Policy** dialog box, click **Let's Do It** to go directly to the workflow.
- Step 4** In the **Define Policy Details** window, do the following:
- Enter a name for your policy in the **Rule Name** field.
 - From the **Select Status** drop-down list, choose **Enabled** or **Disabled**.
 - Define the time of inactivity after which an endpoint must be purged. Enter a value (in days) in the **Elapsed Greater than or Equal to** field. The accepted value range is from 5 to 180 days.
- Step 5** (Optional) In the **Define Additional Policy Conditions** window, choose the profiling attributes, to filter the endpoints that are impacted by this purge policy. Check the check box next to the attribute you want to select and choose the required values from the drop-down lists displayed for the attribute.
- Step 6** The **Summary** window displays your Purge Policy configuration. Review the details that are displayed and click **Done** to create the policy.
-

What to do next

Audit Logs of Endpoint Purge Activities

After you enable an Endpoint Purge Policy and a purge activity is executed, you can view the audit logs. For more information, see **View Audit Logs** in the [Cisco DNA Center Administrator Guide](#).

Configure Endpoint Subnet Inspection

In a deployment, devices at the access layer and devices above the access layer have different IP subnets. In the case of Cisco TTA devices, endpoint profiling accuracy is optimum when only southbound traffic is analyzed by Cisco AI Endpoint Analytics. To allow better endpoint profiling, configure specific IP subnets or subnet ranges that must be analyzed by Cisco AI Endpoint Analytics.

This configuration of filtered subnets is then shared with Cisco SD-AVC servers. The configuration is applied on Cisco TTA devices though Cisco SD-AVC servers.

- Step 1** Click the menu icon (☰) and choose **Policy > AI Endpoint Analytics > Configurations > Endpoint Subnet Inspection**.
- Step 2** Enter the required value in the **IP Subnet** field.
- Step 3** Click + to add another IP subnet. You can add multiple subnets or subnet ranges in this window.
-

Endpoint Inventory

The **Endpoint Inventory** tab displays details of the endpoints that are connected to Cisco AI Endpoint Analytics through the configured data sources. This view displays the profiling information of all the connected endpoints.

To select the profiling information you want to view for the endpoints, click the vertical ellipsis icon at the top-right corner of the table. Choose one of the following sets of profiling information and click **Apply**:

- **All**: All the profiling information that is available is displayed. You cannot edit this set.
- **General**: This is a selection of profiling information that gives you a generic view of the endpoints. This is the set of columns that are displayed by default. You cannot edit this set.
- **Detailed**: This is a selection of profiling information that provides a deeper view of the endpoints. You cannot edit this set.
- **Custom**: This is the only set that you can edit. Check or uncheck the profiling information that you want to view in the **Endpoint Inventory** window.

You can also filter the list endpoints that is displayed in the **All Endpoints** view by clicking the required **View Known Profiles** buttons. You can filter the list of endpoints by **Endpoint Type**, **Hardware Manufacturer**, **Hardware Model**, and **OS Type**.

To edit or customize the endpoint inventory table that is displayed, click the gear icon in the right corner at the top of the table. The pane that is displayed contains the **Table Appearance**, **Edit Table Columns**, and **Edit Custom Views** menus where you can choose a table view, the information that you want displayed in the table, and create custom views.

Click **Apply** to save the changes, or click **Reset All Settings** to apply the default settings for the endpoint inventory table.

You can easily filter a set of endpoints based on your requirement. The search bar at the top of table allows you to easily find a filter parameter. You can type and use the assisted search feature, or you can scroll the drop-down that is displayed to find and select the required parameters.

Most of the columns contain quick filters. While some filters display drop-down menus for you to choose values from, some filters are text fields you can type into.

You can register endpoints, and edit, delete, and profile the registered endpoints. You can select single or multiple endpoints by checking the check box near the MAC addresses to filter and perform a particular action on the chosen endpoints from the **Actions** drop-down list.

You can delete registered endpoints, unregistered endpoints and endpoints learnt from other sources as well. When you select an endpoint, a banner row is displayed that allows you to select all the rows in the table. When you click on the banner, the banner row now allows you to clear all the rows in the table. To delete all the endpoints, you can click on the banner or choose the **Delete** option from the **More Actions** drop-down list.

To see the complete profiling details of an endpoint, click the **MAC Address** of the endpoint. A slide-in dialog box is displayed which contains user details, endpoint details, and attribute details of the endpoint.

In the **Details** tab, the following new fields are displayed in Cisco DNA Center 2.2.2 and later, with the details received from Cisco ISE:

- **Authentication Status:** This field displays **Started** when an endpoint is authenticated through Cisco ISE, and **Disconnected** when it is not.
- **Authorization Profile:** The authorization policies configured for an endpoint in Cisco ISE are displayed here.
- **Security Group Tag:** The Security Group Tags configured for an endpoint in Cisco ISE are displayed here.

For information on these attributes, see the [Cisco ISE Administrator Guide](#) for the Cisco ISE release that you use.

In Cisco DNA Center 2.2.2 and later, the **Trust Score** tab is available in the slide-in dialog box for endpoint details. This tab displays details of the various factors that inform trust score of an endpoint. See [Trust Scores for Endpoints, on page 646](#).

In Cisco DNA Center 2.2.3 and later, the **Details** tab contains the **Previous MAC Addresses** area, which displays the MAC addresses that have been used by an endpoint which has the MAC Randomization feature enabled on it. See [Trust Scores for Endpoints with Random and Changing MAC Addresses, on page 652](#).

Export Cisco AI Endpoint Analytics Data

To export a list of endpoints and their details from this window, click **Export**. If you apply any filters in the **Endpoint Inventory** window, only the filtered endpoints will be processed for export. To export the details of all the endpoints, ensure that no filters are applied when you click **Export**.

When you click **Export**, a new tab opens with the **Reports** window. The **Generated Reports** window contains a list of exports initiated, with the latest export request at the top of the list. A report generated from the Endpoint Inventory window contains **AI Endpoint Analytics** in its **Template Category** column. Report generation takes a few minutes. When a report is ready for download, the value in the **Last Run** column changes from **Not Initiated** to a timestamp with a download icon next to it. The timestamp refers to the time at which the export list was generated. Click the download icon to download a CSV file of the list of endpoints to your system.

You can also export Cisco AI Endpoint Analytics data from the **Reports** window, through the following steps:



Note You must run your first export of AI Endpoint Analytics data for endpoints from the **Endpoint Inventory** window. Then you can generate AI Endpoint Analytics reports directly from the **Reports** window.

Step 1 Click the menu icon (☰) and choose **Reports > Report Templates > AI Endpoint Analytics**.

Step 2 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Note To skip this screen in the future, check the **Don't show this to me again** check box.

Step 3 In the **Select Report Template** window, the template **Endpoint Profiling** is applied by default.

Step 4 In the **Setup Report Scope** window, do the following:

- Enter a name in the **Report Name** field.
- Define the filters that you want to apply to the list of endpoints that you want to export from the **Endpoint Inventory** window.

c) To export the details of all endpoints, do not choose any values in the **Scope** area.

Step 5 In the **Select File Type** window, the **Client Details** area allows you to review the chosen parameters. Edit the information to be exported by checking or unchecking the check boxes next to the relevant fields.

Step 6 In the **Schedule Report** window, click **Run Now**, **Run Later (One-Time)**, or **Run Recurring** radio button.

Note The **Run Later (One-Time)** and **Run Recurring** options display scheduling fields to define the time of export.

Step 7 In the **Delivery and Notification** window, do not check the **Email Report** check box.

Step 8 In the **Summary** window, review all the configurations. To make any changes, click **Edit**.

Step 9 Click the **View Reports** link in this window for a list of generated reports. It takes a few minutes for the report to be generated and displayed in this window.

Filter Endpoints

Use this procedure to filter the endpoints based on their profiling data, primary profiling labels, known profiles, and health status.

Step 1 In the **Endpoint Inventory** window, click **Filter**.

Step 2 Define the following filters by choosing a value from the corresponding drop-down list, clicking the radio button for the required value, or checking the check box next to the required value for a particular field as applicable:

- **Profile Status Condition**
- **Mac Address**
- **Is Random Mac**
- **Trust Score**
- **IP Address**
- **Last Seen**
- **Host Name**
- **Endpoint Type**
- **OS Type**
- **Hardware Model**
- **Hardware Manufacturer**
- **Registered**

Step 3 Click **Apply**.

You can also filter the profiled endpoints displayed by the four primary profiling labels. Click one or more of the labels in the **View Known Profiles** section.

The health status of endpoints is updated every five minutes.

Attribute Glossary

Attribute glossary is a list of all the profiling attributes available from Cisco ISE probe data.

In order to view all the profiling attributes, follow the below steps.

Step 1 In the **Endpoint Inventory** window, click the MAC address of an endpoint.

Step 2 In the new area that is displayed on the right side, click **View Attribute Glossary**.

The **Attribute Glossary** window displays the following information for each attribute:

- **Key profiling attributes**
- **Description**
- **Associated Profile Labels**
- **Source**
- **Dictionary**
- **Discovery Method**

The glossary gives you a detailed view of all the profiling attributes. If a profiling attribute is frequently used to create a profile label, the label is listed in the **Associated Profile Labels** column.

You can also view the attribute glossary in the **Choose Attribute Condition** window while creating a logical condition for the rules. For more information, see [Create a Custom Rule](#).

Register Endpoints

You can onboard and profile new endpoints by registering them in Cisco AI Endpoint Analytics. The profiling information of an endpoint is the source of truth for classification. You can also update new profile information for a registered endpoint using the **Register Endpoint** option.

Step 1 Choose **Actions > Register Endpoints**.

Step 2 Choose whether you want to register a single endpoint or multiple endpoints, by clicking the **Single** or **Bulk** radio button.

- a) Click **Single** radio button, enter the **MAC Address**, **Endpoint Type**, **Hardware Model** and **Hardware Manufacturer** for the endpoint.
- b) Click **Bulk** radio button and do the following:
 1. Download a .csv template by clicking the **Download .csv Template** option.
 2. In the downloaded .csv file, enter the following details for each endpoint you must register: MAC address, endpoint type, hardware model, and hardware manufacturer. Save this file.
 3. Upload the .csv file using the **Choose a File** option.

You can register a maximum of 500 endpoints at a time using the **Bulk** option.

Step 3 In the **Review Endpoint** window, review the endpoint details. To make any changes, click **Edit**.

Note While registering an existing endpoint, the profile label changes of the endpoint are reflected in purple color and can be edited.

Step 4 Click **Next** to continue with the registration process.

Step 5 Click **Register**.

Edit Registered Endpoints

You can update the profiling information of registered endpoints from the **Endpoint Inventory** window.

Step 1 Check the check box adjacent to the MAC address of the endpoint that you want to edit.

Step 2 Click **Actions**.

Step 3 Click **Edit Endpoint**.

Step 4 Enter the **Endpoint Type**, **Hardware Model**, and **Hardware Manufacturer** details.

Step 5 Click **Save**.

Delete Registered Endpoints

If there are registered endpoints that are no a longer part of your network, you can delete them from Cisco AI Endpoint Analytics.

Step 1 Check the check box adjacent to the MAC address of the endpoints that you want to delete.

Step 2 Click **Actions**.

Step 3 Click **Delete Endpoint**.

The following message is displayed:

Do you really want to delete the selected endpoint(s)?

Step 4 Click **Yes** to permanently delete the endpoint from Cisco AI Endpoint Analytics.

Trust Score

The Trust Score window consists of two tabular sections:

Alerts:

Alerts appear when there is a deviation caused by anomalies or vulnerabilities, or when a weakness is identified in endpoint connections or interfaces. These alerts reflect a detection that has a negative impact on the trust

score (such as concurrent MAC address detection, NAT mode, or other untrustworthy changes). You can monitor the alerts to quickly address the most urgent risks within your network.

The **Alerts** tab displays the various alerts received by the endpoints in the network. Earlier you had to individually check the details for each endpoint to see the type of alerts the endpoint has received and there was no way to know what other endpoints have received the same alert. Now, you have the capability to know all the endpoints that have received a particular type of alert. You can click on any alert to view the list of endpoints that have received this alert. You can further click on each endpoint to see the details. The alerts can be in any of the following three states:

- **Open:** An alert is in the open state when the alert is initially detected for an endpoint and an action is required from your side to resolve the alert or address it later.
- **Disabled:** If you do not want to take any action on an open alert, you can move it to the disabled state. You can disable the alert for any time period and even indefinitely. During this time period, the alert remains in the disabled state even if any new endpoints are detected with this alert.
- **Reset:** If you do not want to take any action on an alert right away, you can move it to the reset state. When this alert is detected on another endpoint after resetting, the alert is brought back to the open state.

Endpoint:

This view displays columns for the various factors that inform the overall Trust Score of an endpoint. The Trust Score helps you identify the endpoints in which behavioral anomalies have been detected, so you can examine the details of the endpoint and take the necessary remediation actions. If you apply an ANC policy to an endpoint to manage its low Trust Score, the Trust Score view also displays the name of the ANC policy applied and when the policy was applied. See [Trust Scores for Endpoints, on page 646](#).

Using the option **Reset Trust Score**, you can now reset multiple endpoints at the same time with an upper limit of 10 endpoints to avoid any performance issues. While resetting the endpoints, a justification is required for the action for audit purposes. Once an endpoint is reset, the endpoint is cleared of its trust score and any ANC policy that was applied to it.

Trust Scores for Endpoints

Cisco AI Endpoint Analytics assigns Trust Scores to endpoints to allow you to easily monitor and act on potentially risky endpoints in your network. Behavioral anomalies are monitored and tracked, and a Trust Score is assigned based on the number and frequency of the anomalies tracked.

To choose the sources that must be included in the calculation of Trust Scores, from the Cisco AI Endpoint Analytics **Overview** window, choose **Configuration > Trust Analytics**. Click on a source to open its slide-in configuration window on the right. Click the toggle button to enable the source.

Cisco AI Endpoint Analytics generates historical Trust Scores based on the following factors:

- The history of anomalies associated with an endpoint—how many anomalies have been detected for this endpoint?
- The severity of each anomaly detected for the endpoint.

In Cisco DNA Center 2.2.3 and later, the overall Trust Score calculation for an endpoint factors in the following anomalies and scores are displayed for each anomaly that is detected (if the corresponding source is enabled):

- **AI Spoofing Detection**

Cisco AI Endpoint Analytics analyzes NetFlow telemetry data, and network probe data from Cisco ISE and SD-AVC devices, to detect spoofed endpoints. For more information on how to configure NetFlow Collector servers, see [Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 27](#). In Cisco DNA Center 2.3.2 and later, probe and NetFlow data from Cisco DNA Traffic Telemetry Appliances (DN-APL-TTA-M) is also analyzed. Configure inbound span of traffic toward your Cisco DNA Traffic Telemetry Appliances so the endpoint traffic data is then available to Cisco AI Endpoint Analytics for spoofing detection.

Each endpoint type has a behavior model that is developed using machine learning algorithms. Based on the data received for an endpoint, if an endpoint's behavior is unexpected of its endpoint type profile, the endpoint is assigned a low Trust Score in the AI Spoofing Detection area. The applications and server ports that are used by an endpoint are analyzed in this spoofing detection process. For example, if an endpoint profiled as a printer uses a video calling application, it is identified as a spoofed endpoint and assigned a Trust Score.

Endpoints are identified by their MAC addresses on a Cisco DNA Center-managed switch. Several endpoints using a single MAC address such as by using NAT, running a virtual machine or a container, is not a supported configuration on Cisco AI Endpoint Analytics.

AI Spoofing Detection currently covers the following device types:

- IP Phones
- Printers
- Cameras
- Building automation devices with the following hardware model attributes:
 - Automated-Logic-Device
 - Honeywell-Device
 - Johnson-Controls-Device
 - Rockwell-Automation-Device
 - Schneider-Electric-Device
 - Siemens-Automation-Device
 - Siemens-Building-Device
 - Trane-Device
- Telepresence:
 - Endpoints with one of the following hardware models:
 - Cisco-Tandberg-Device
 - Cisco-TelePresence
 - Cisco Telepresence SX80
 - Cisco Telepresence SX20
 - Cisco-Collaboration-Room-Endpoint
 - Poly-Device

- Endpoints with the device type Video Conferencing

- **Endpoint Attribute Conflict**

When a device joins a network, and then through periodic probing while the device is active, the profiling data for an endpoint is continuously monitored and updated. Certain changes in the profiling data that is received from an endpoint are flagged as anomalies in Cisco AI Endpoint Analytics. For example, if an endpoint was first profiled as a Linux device and is then profiled as a macOS device, this is flagged as a high-severity anomaly. A score is assigned in the Endpoint Attribute Conflict column for the endpoint and the endpoint's overall Trust Score is also updated to reflect this change.

However, if there is a change in the version of macOS and the endpoint appears to have downgraded from a later release to an earlier release, such a change is flagged as a lower priority anomaly and the corresponding scores are updated accordingly.

- **NAT Mode Detection**

If you have a NAT-enabled router in your network, an endpoint that is connected to a NAT router is recognized by the IP or MAC addresses of the router instead of the IP or MAC addresses of the specific endpoint. Information on NAT-enabled routers is collected from the Cisco Catalyst 9000 Series devices they are connected to.

- **Concurrent MAC Addresses**

Identify the endpoints that share the same MAC addresses and are connected to Cisco Catalyst 9000 Series devices. The endpoints with shared MAC addresses are assigned a Concurrent MAC Address score, and you can easily identify these endpoints and examine their details.

- **Security Sensor**

With the Security Sensor scan feature, you can install active probes on specific Cisco Catalyst 9000 Series switches, and configure Cisco AI Endpoint Analytics to scan endpoints for open ports that are not expected to be open, for credential vulnerabilities or both.

The Trust Score of an endpoint is also informed by the following events that are collected from Cisco ISE. Every endpoint that authenticates through Cisco ISE receives an initial Trust Score based on the following events:

- **Authentication Method**
- **Posture**



Note For the Trust Score sources that receive data from Cisco Catalyst 9000 Series devices, you must enable CBAR on the devices and upgrade the devices to Cisco IOS-XE Release 17.6 or later.

The Trust Score that is displayed in the **Endpoint Inventory** window is the overall trust score that takes the history and severity of anomalies for an endpoint. Click the **MAC Address** to view the details of the causes for the Trust Score that is assigned to an endpoint. This means that if a low-level anomaly was detected for an endpoint, and this is the only instance of an anomaly, the overall Trust Score for the endpoint would be a 9.

If multiple low-level anomalies are detected, the overall Trust Score would further decrease to account for the number of anomalies.

The trust scores assigned range from 1 through 10, and are categorized as follows:

Trust Score Category	Range	Threat Level of Endpoint
Low	1–3	High
Medium	4–6	Moderate
High	7–10	Low

You can then apply Adaptive Network Control (ANC) policies from Cisco ISE to enforce appropriate remediation actions on the endpoints. See section “Adaptive Network Control” in Chapter “Cisco ISE Admin Guide: Maintain and Monitor” of the *Cisco ISE Administrator Guide*.

The ANC policies are defined in Cisco ISE and allow you to apply remediation actions on chosen endpoints. You can apply ANC policies to quarantine, shut down, or port bounce an endpoint, or force endpoint reauthentication. When you apply an ANC policy to an endpoint with an undesirable Trust Score in Cisco AI Endpoint Analytics, a Change of Authorization (CoA) is sent to the endpoint from Cisco ISE.

An endpoint is identified by its MAC address. Cisco ISE sends the CoA to the endpoints that hold an active session for the identified MAC address at the time of the ANC application. Any endpoint with the same MAC address that does not have an active session in Cisco ISE at the time matches the ANC policy when a new session starts or when it must reauthenticate at the end of the configured reauthentication timer.

To verify which endpoint is being acted upon by the ANC policy, log in to your Cisco ISE administration portal. From the main menu, choose **Operations > RADIUS > Live Sessions**. Enter the MAC address of the spoofed endpoint in the **Endpoint ID** column, to filter the endpoints that share the same MAC address and currently have live sessions in Cisco ISE. These are the endpoints that will be affected by the ANC policy.

To view a historic log of the RADIUS sessions in Cisco ISE, from the main menu, choose **Operations > Reports > Reports > Endpoints and Users > RADIUS Authentications**.

To view or modify ANC policy application on endpoints in Cisco ISE, from the main menu, choose **Context Visibility > Endpoints**. Check the check box next to the MAC address of an endpoint and click the options that are displayed at the top of the list, as required.

Prerequisites

Prerequisites for receiving Trust Scores for endpoints:

- Cisco DNA Center is upgraded to Release 2.2.2 or later.
- Cisco ISE is connected to your on-premises Cisco DNA Center.
- Network access devices are managed by both Cisco DNA Assurance and Cisco ISE.



Note The endpoint spoofing detection feature supports a maximum of 500 network access devices with NetFlow export flows, as Cisco DNA Assurance supports only 500 NetFlow exporters.

- Endpoints connected to network access devices are authenticated through Cisco ISE.
- Enable the required sources for Trust Score calculation in the Trust Score Sources window (**Policy > AI Endpoint Analytics > Configurations > Trust Analytics**).

Endpoint Attribute Conflict

Cisco AI Endpoint Analytics collects data from multiple probes from different sources continually to derive accurate profile labels for endpoints. Cisco AI Endpoint Analytics collects the following data from the following sources:

From Cisco ISE:

- RADIUS probes.
- User details from Directory.
- VPN details like AnyConnect availability.
- Optionally, other data if port forwarding is configured. For example, DHCP details.

From switches:

- Device connection messages. For example, DHCP and NetBIOS messages.
- Deep packet inspection
- Switch telemetry

Cisco AI Endpoint Analytics creates system rules based on the information received from these sources. When a device joins a network, and then through periodic probing while the device is active, the profiling data for an endpoint is continuously monitored and updated.

Certain changes in the profiling data received from the endpoint are flagged as anomalies in Cisco AI Endpoint Analytics. For example, if an endpoint was first profiled as a Linux device and is then profiled as a macOS device, this is flagged as a high-severity anomaly. A score is assigned in the Endpoint Attribute Conflict column for the endpoint and the endpoint's overall Trust Score is also updated to reflect this change.

However, if there is a change in the sub-version of macOS and the endpoint appears to have downgraded from a later release to an earlier release, such a change is flagged as a lower priority anomaly and the corresponding scores are updated accordingly.

In the **Endpoint Inventory** window, click the MAC Address of an endpoint with a **Endpoint Attribute Conflict** score to view the profiling data changes recorded. The old and new profiles for the endpoints are displayed here. If the profiling changes are not of concern for any reason, or if you think the profiling change detected is erroneous, reset the score by clicking the corresponding button in the **Endpoint Attribute Conflict** area of the endpoint's details.

You can also disable Endpoint Attribute Conflict detection for a specific endpoint by clicking the toggle button in the Endpoint Attribute Conflict area of the endpoint's details.

Data regarding this anomaly is sent to Cisco ISE if the affected endpoint is connected to Cisco ISE. The data is available as an Endpoint Analytics dictionary attribute that a Cisco ISE administrator can easily use to define policies.

Endpoint Attribute Conflict detection is not available for the endpoints that have Custom Rules applied to them.

NAT Mode Detection

Network Address Translation (NAT) allows private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT can be configured to advertise to the outside world only one address for the entire network. If you have a NAT-enabled router in your network, an endpoint connected to a NAT router

is recognized by the IP or MAC addresses of the router instead of the IP or MAC addresses of the specific endpoint. Information on NAT-enabled routers is collected from the Cisco Catalyst 9000 Series devices they are connected to.

NAT detection is included in Trust Score calculation as a device acting as a NAC-enabled router could allow unauthorized endpoints to connect to your network. For the endpoints that are assigned a NAT Mode Detection score, in the **Endpoint Inventory** tab, click the MAC Address to view the details of the endpoint in a slide-in window. If you are certain that the identity of the endpoint corresponds to a NAT-enabled router in your network:

1. Click **NAT Mode Detection** in the Trust Score tab of the details slide-in window.
2. Click the toggle button to disable NAT Detection for this specific endpoint.

Endpoints with Concurrent MAC Addresses Connected to Cisco Catalyst 9000 Series Devices

Identify the endpoints that share the same MAC addresses and are connected to Cisco Catalyst 9000 Series devices. The issue of endpoints with concurrent MAC addresses occurs in wired environments and in hybrid environments that contain wired and wireless deployments. In a wireless environment, concurrent MAC addresses do not occur as only one endpoint with a specific MAC address is allowed to access the network at any time.

Cisco AI Endpoint Analytics allows you to identify the endpoints with concurrent MAC addresses by assigning a Concurrent MAC Address score to the endpoints. To detect endpoints with shared MAC addresses in your network, you must enable CBAR in the connected Cisco Catalyst 9000 Series devices.

When devices with the same MAC Address connect to a Cisco Catalyst 9000 Series device, the endpoints are recognized as concurrent endpoints and a low score is assigned to the MAC Address. Endpoints with concurrent MAC addresses may be connected to:

- The same Cisco Catalyst 9000 Series device from different VLANs
- Different Cisco Catalyst 9000 Series devices

Table 47: Environments in Which the Concurrent MAC Address Issue Occurs

Deployment 1	Deployment 2	Can Concurrent MAC Addresses Occur in the Network?	Concurrent MAC Addresses Detection Support in this Environment
Wired	Wired	Yes	Yes
Wired	Wireless	Yes	Yes
Wireless	Wired	Yes	Yes
Wireless	Wireless	No	No

In Cisco DNA Center Release 2.2.3 and later releases, the **Trust Scores** view of the **Endpoint Inventory** tab contains the **Concurrent MAC Address** column. Shared MAC addresses are detected as an anomaly and a low score is assigned in the **Concurrent MAC Address** column. Click the MAC Address to view a slide-in window with the details of the MAC Address. Click **Concurrent MAC Address** and the field expands to display information regarding the various sources of the MAC address.

In the **Concurrent MAC Address** area, the **Network Device Name** column displays the name of the Cisco Catalyst 9000 Series device to which an endpoint is connected. The **Interface** and **VLAN** columns display the corresponding values to help you identify how the endpoint is connected to the network.

Initial Trust Score Assessment Using Posture and Authentication Values from Cisco ISE

When an endpoint authenticates through Cisco ISE, a Trust Score is immediately assigned to the endpoint based on its authentication and posture details. Authentication Method score is assigned by default and you cannot disable or act upon this score. You can choose to enable or disable Posture-based scores, either at a global level from the **Configurations** window, or for a particular endpoint in the **Endpoint Inventory** tab. The Trust Score that is assigned based on the Authentication Method and Posture values becomes the initial Trust Score for the endpoint.

Any other anomalous behaviors detected for this endpoint would then impact this initial Trust Score and drive it lower based on the severity and number of the anomalies.

The **Authentication Method** score, displayed in the details of an endpoint in the **Endpoint Inventory** tab, is based on the perceived security level of the authentication method used. For example, WebAuth Over HTTPS, certificate-based authentication, and authentication using secure tunnels receive high Trust Scores.

The **Posture** score is based on whether or not the connect endpoint is posture compliant.

If an endpoint's Trust Score consists of only the Authentication Method score, the **Reset Trust Score** button is inactive. When a Trust Score source other than the Authentication Method displays a score, you can use the reset option.

Trust Scores for Endpoints with Random and Changing MAC Addresses

As a privacy measure, mobile devices increasingly use random and changing MAC addresses for each SSID that they connect to. Some desktop operating systems offer users the ability to randomize MAC addresses at regular intervals as well. This means that an endpoint presents different MAC addresses every time they connect to a different SSID.

Cisco AI Endpoint Analytics enables you to handle the issue of random and changing MAC addresses by receiving from Cisco ISE a unique endpoint identifier called the DUID (also known as GUID in Cisco ISE). Cisco AI Endpoint Analytics then uses the DUID as the identifier for an endpoint, instead of its MAC address. For more information how GUIDs are assigned in Cisco ISE, see Cisco ISE Administration Guide, Release 3.1.

The Endpoint MAC Randomization dashlet in the Cisco AI Endpoint Analytics **Overview** window displays a graphical representation of how many endpoints in your network are using random and changing MAC addresses.

For the endpoints that are connected to Cisco ISE and have DUID information available, this information is displayed in Cisco AI Endpoint Analytics as well. The following columns display the required information in the **Endpoint Inventory** window in Cisco AI Endpoint Analytics:

- **DUID:** The DUID value for the endpoint.
- **Previous MAC Addresses:** The random and changing MAC addresses with which the endpoint previously connected to the network.

Using the DUID value, Cisco AI Endpoint Analytics is now able to reliably identify an endpoint and track the various MAC addresses that the endpoint has previously used. This means that the Trust Score for an endpoint with random and changing MAC addresses still has high fidelity. The Trust Score of the endpoint

from a previous MAC addresses is carried forward to the current MAC address that the endpoint is presenting and continues to be impacted by the probe data received for the same endpoint.

If a device has the **Private Address** setting enabled, the **Is MAC Random** column for this device displays the value **Yes**. This device is then recognized as a random and changing MAC address. However, whether or not a DUID value is available for this device depends on whether or not the endpoint was authenticated through Cisco ISE and if a GUID was generated for this endpoint in Cisco ISE.

Sensor Scans to Check for Open Ports and Credential Vulnerabilities

Install an active probes container to gain more information about the endpoints in your network. When you enable security sensor scans, the Trust Score that is assigned to an endpoint takes into account any anomalies in open ports and endpoint login credentials.

The sensor scan feature is supported by the following switches:

- Cisco Catalyst 9300 Series switches
- Cisco Catalyst 9400 Series switches



Note Cisco Catalyst 9800 Series Wireless Controllers do not support the sensor scan feature.

Cisco AI Endpoint Analytics uses the Application Hosting capability that is available on the switches to enable scans for open ports and weak credentials.

Enable and Monitor Sensor Scans

Before you begin

- Connection to Cisco ISE Release 3.1 or later releases, if you want to enforce endpoint policies based on the scan results.
- Connection to Cisco Catalyst 9300 or 9400 Series devices.
- Ensure that the switches are upgraded to Cisco IOS XE Release 17.7.1 or later releases.

-
- Step 1** Log in to your Cisco DNA Center.
- Step 2** From the main menu, choose **Policy > AI Endpoint Analytics**.
- Step 3** In the **Overview** window that is displayed, click **Configurations**.
- Step 4** From the left pane, choose **Trust Analytics**.
- Step 5** In the **Security Sensor** area, the prerequisites for using the sensor scans feature to identify open ports and weak endpoint credentials are displayed. Click the corresponding links in this area to carry out the following tasks:
- a. Verify the supported Cisco DNA Center and Cisco IOS-XE releases from the release notes for Cisco Catalyst 9000 Series devices. Download the security sensor container from software.cisco.com for the relevant Cisco Catalyst 9000 Series device. A .tar file downloads to your system.
 - b. Install App Hosting in your Cisco DNA Center. See [Application Hosting, on page 529](#) for instructions.
 - c. Upload the .tar file in your Cisco DNA Center App Hosting window. The link to the App Hosting window is displayed in the **Security Sensor** area.

- d. Install and enable the .tar file in each Cisco Catalyst 9000 Series device that you want to enable sensor scans on.

In your Cisco DNA Center App Hosting window, check that the **App Hosting Status** is active for least one of the Cisco Catalyst 9000 Series devices on which you enabled the .tar file.

Step 6 After the active probes container is installed and enabled as explained in the previous step, in the **Security Sensor** area, you can configure Trust Score settings in Cisco AI Endpoint Analytics to scan for open ports and weak credentials on endpoints that are connected to Cisco ISE and the Cisco Catalyst devices on which the active probes application is enabled.

- Click the **Open Port Scan** toggle button to enable Cisco AI Endpoint Analytics to proactively run port scans to detect and close possible vulnerabilities on defined endpoints on the network.
- Click the **Credential Vulnerability Scan** toggle button to enable Cisco AI Endpoint Analytics to proactively detect when endpoints on your network are using weak credentials in order to prevent malicious activity.

Step 7 (Optional) If you choose to enable scanning for open ports, you can define the scan by clicking **Scan Configuration** in the **Open Port Scan** area.

- a) In the **Scan Configuration** window, in the **Defined Scans** tab, click the **Define Scan** button.
- b) A dialog box is displayed that allows you to define the scope of a port scan:
 - To scan each endpoint at the time of endpoint enrollment, choose the **On enrollment, scan all endpoints** radio button.
 - To define the scope of the open port scan by subnet, profiling attributes, and more, choose the **Create a Custom Scan** radio button.

In both types of port scan, you define a list of unauthorized ports to specify the ports that must always be closed. This list allows Cisco AI Endpoint Analytics to recognize anomalous port activity on an endpoint and assign it a low trust score. For both port scan types, the minimum frequency of scan that you can configure is 12 hours.

- c) In the **Scan Configuration** window, in the **Open Ports List** tab, specify the type and range of ports, or individual ports, that must be scanned.
- d) In the **Scan Configuration** window, in the **Unauthorized Ports** tab, define by port number and port type, the ports that are unauthorized in your network. If Cisco AI Endpoint Analytics detects these ports as active, the endpoint is given a low trust score for the anomaly of an active unauthorized port.

Step 8 (Optional) If you choose to enable the detection of weak credentials, you can define the scan by clicking **Scan Configuration** in the **Credential Vulnerability Scan** area. SSH and TELNET protocols are supported by this feature.

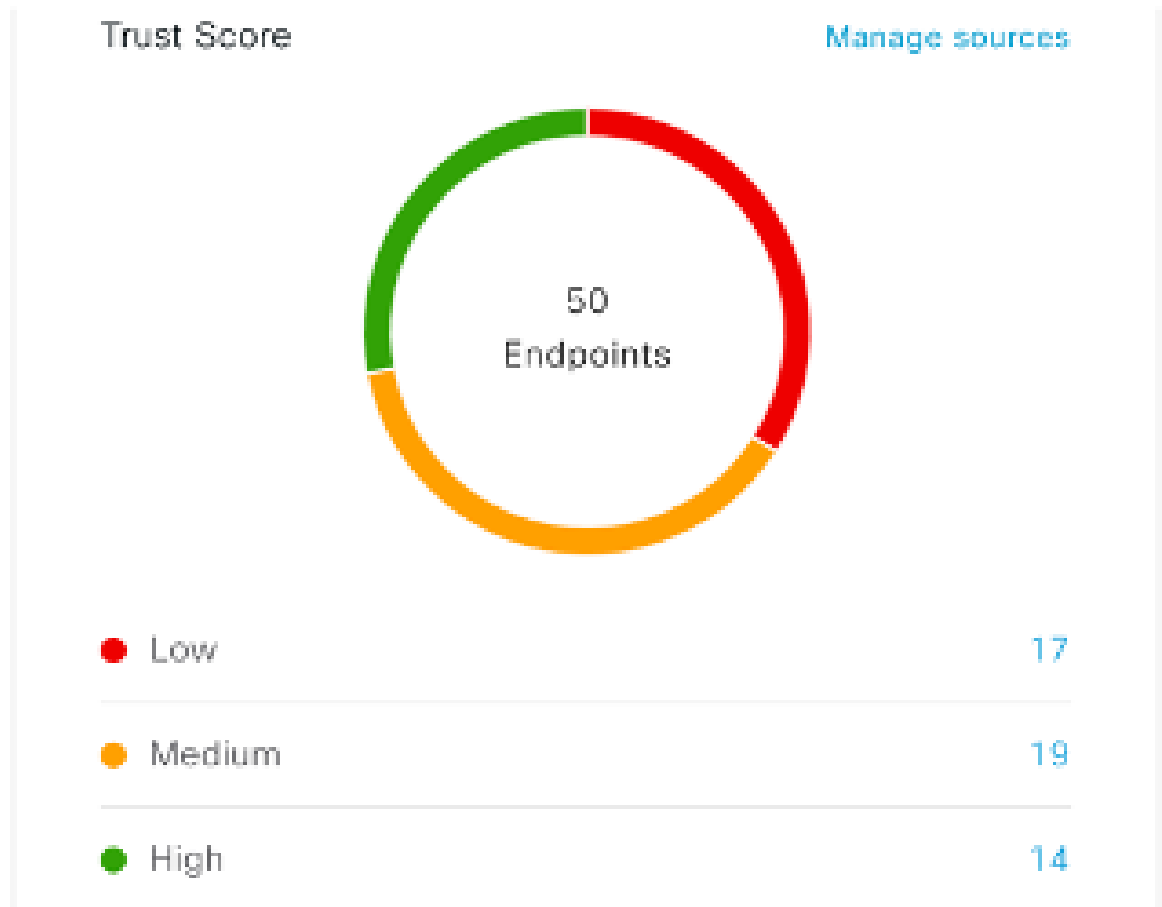
- a) In the **Credential Vulnerability Scan** window, in the **Scan** tab, define a list of credentials that you want to identify as weak credentials. Define lists of usernames and passwords that are considered vulnerable according to your enterprise requirements.
- b) In the **Credentials** tab, a default list of more than 3500 weak credentials is available by default. You can use this default list to create a credential vulnerability scan. To add a new list of vulnerable credentials, click **Create New List**.

The minimum frequency of credential vulnerability scan that you can configure is 12 hours.

Step 9 For the scans that you enable in the **Security Sensor**, the relevant endpoints are scanned and if anomalies are detected in open ports or credential checks, the Trust Score for these endpoints is adjusted accordingly. In the **Endpoint Inventory** tab, where applicable, the **Trust Score** tab for an endpoint displays the list of unauthorized ports that are open on the endpoint, or weak usernames, or both.

View and Manage Trust Scores for Endpoints

Figure 30: Trust Score Dashlet in Cisco AI Endpoint Analytics Overview Tab



After Cisco DNA Center is upgraded and necessary Trust Score sources are enabled, the Cisco AI Endpoint Analytics **Overview** tab (main menu > **Policy** > **AI Endpoint Analytics**) displays the **Trust Scores** dashlet. This dashlet contains the following information:

- The total number of endpoints that have been assigned a Trust Score.
- A donut chart and a list of the number of endpoints with low, medium, and high trust scores.

To view the details of endpoints in a trust score category, click its endpoint count in the **Trust Scores** dashlet. The **Trust Score** view of the **Endpoint Inventory** tab is displayed with the appropriate filters applied.

You can view endpoints with Trust Scores in two ways:

- In the **Trust Score** tab, choose the **Endpoints** tab to see all the endpoints with Trust Scores assigned.
- In the **Endpoint Inventory** tab, click **View endpoints in Trust Score View** from the caution message that is displayed, to see endpoints with Low and Medium scores.

You can perform the following actions on endpoints with Trust Scores:

- **Apply an ANC Policy**

×

Apply ANC Policy

Choose an ANC Policy to apply to . Doing so will affect the endpoints accessibility to your network based on the ANC Policy applied.

Apply ANC Policy ⌵ [Don't see a policy you like?](#)

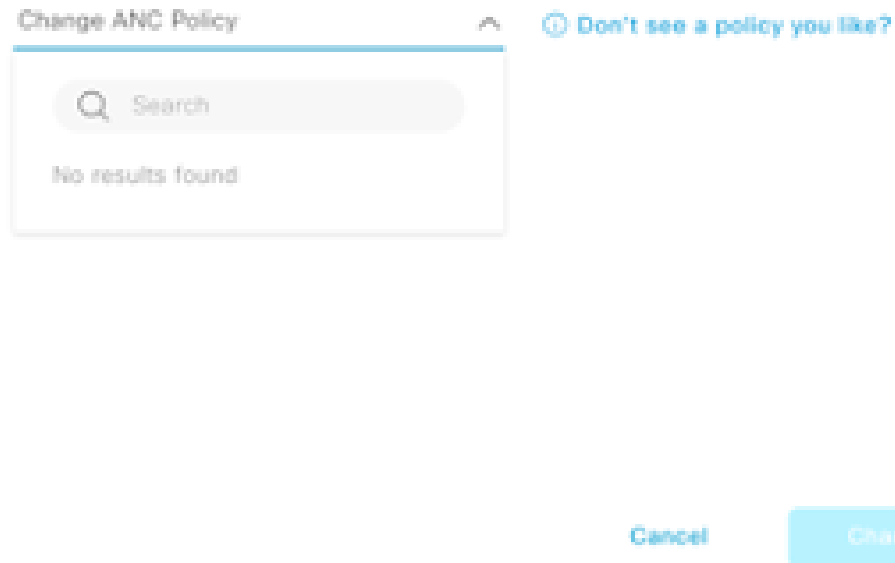
Cancel Apply

Click the **Apply ANC Policy** button to choose an ANC policy to be applied to an endpoint. The endpoint's access to the network is modified accordingly. ANC policies are imported from Cisco ISE and displayed in the drop-down list in the pop-up window displayed.

- **Replace an ANC Policy**

Change ANC Policy

Choose an ANC Policy to apply to 6 endpoints. Doing so will affect the endpoints accessibility to your network based on the ANC Policy applied.



Change ANC Policy

Search

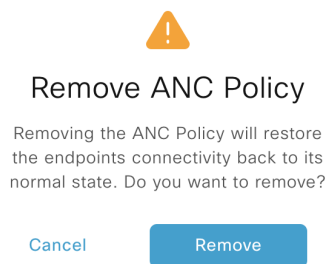
No results found

Don't see a policy you like?

Cancel Change

Click **Change ANC Policy** button to replace an existing ANC policy of an endpoint with another ANC policy. From the pop-up window displayed, choose the new policy to be applied from the **Change ANC Policy** drop-down list.

- **Remove an ANC Policy**



Remove ANC Policy

Removing the ANC Policy will restore the endpoints connectivity back to its normal state. Do you want to remove?

Cancel Remove

Click the **Remove ANC Policy** button to remove an applied ANC policy from an endpoint. In the pop-up window displayed, click **Remove**. This removes the remediation policy that was applied to the endpoint, and allows the endpoint to connect to the network normally.

- **Reset Trust Score**

Figure 31: Reset Trust Score for an Endpoint Without an ANC Policy
Figure 32: Reset Trust Score for an Endpoint with an ANC Policy

Click **Reset Trust Score** button to remove an endpoint from the Trust Score inventory. In the pop-up window displayed, click **Reset**.

If you choose this option for an endpoint after applying an ANC policy, you will not see this endpoint in the Trust Score inventory again. In this case, to modify the ANC policy for such an endpoint, you must remove the policy from Cisco ISE instead.

If you reset the score for an endpoint without applying an ANC policy, you may see the endpoint in the Trust Score inventory again with the next automatic refresh of Trust Score data.

The buttons for each of the actions are displayed in two locations in the **Endpoint Inventory** tab. The actions can be performed on a single endpoint, or on multiple endpoints.

- **Manage Trust Score for Single Endpoint**

Figure 33: Trust Score Options for an Endpoint Without an ANC Policy

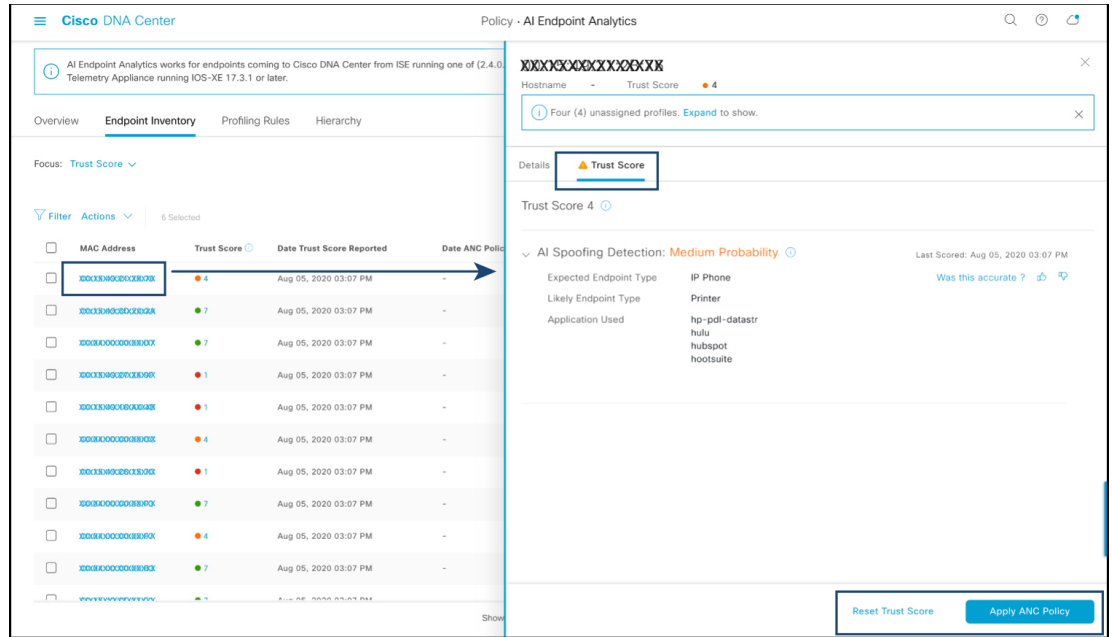
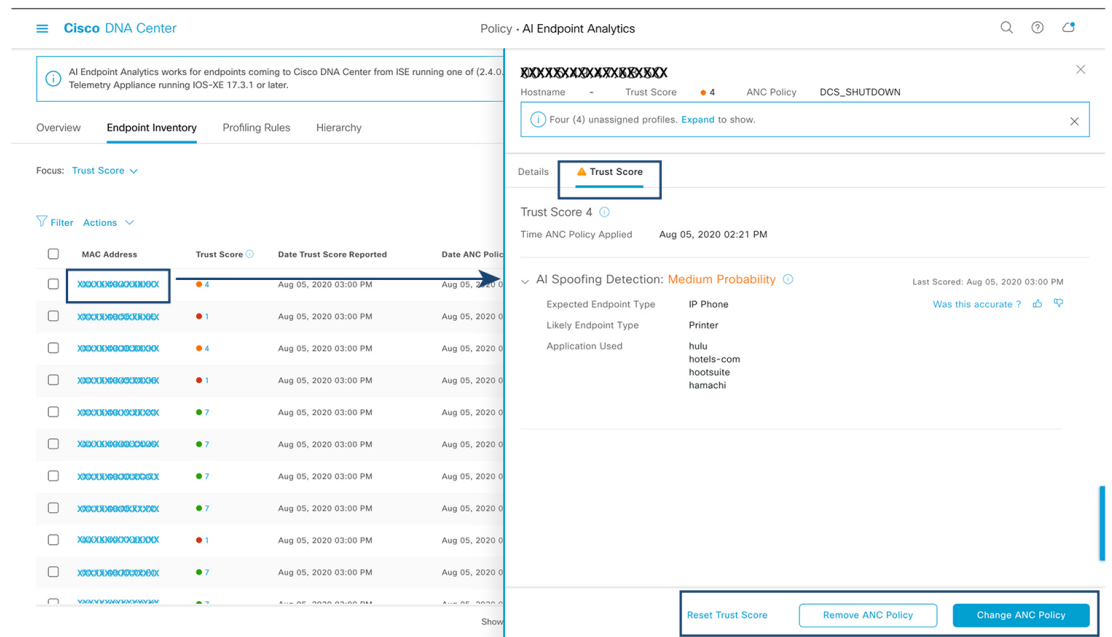


Figure 34: Trust Score Options for an Endpoint with an ANC Policy



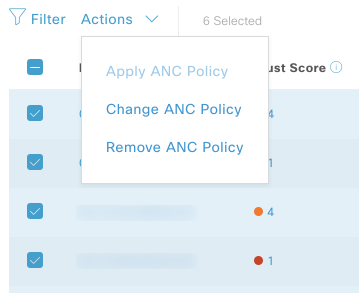
From the list of endpoints with a Trust Score, click the MAC Address of the endpoint you want to manage. In the endpoints details pane that is displayed, click the **Trust Score** tab.

Here, **Expected Endpoint Type** value is displayed. The **Applications Used** field lists the applications that are used by the endpoint.

This pane includes buttons to start the workflows of accepting and removing ANC policies, and to reset the Trust Score. Click the button for the intended task.

Alternatively, you can check the check box for an individual endpoint on the **Endpoint Inventory** window, click **Actions**, and choose the required option from the drop-down list.

- **Manage Trust Score for Multiple Endpoints**



In the **Endpoint Inventory** tab, check the check boxes for all the endpoints you must perform a specific action on. Click **Actions** and choose the required action from the drop-down list.

Control Endpoint Spoofing

Concurrent MAC address detection means that two endpoints with the same MAC address are detected accessing the network and generating traffic. It then becomes imperative to distinguish between the real endpoint and the spoofed endpoint and take the necessary remediation action for the spoofed endpoint.

The Control Endpoint Spoofing feature provides granular policy control by providing network information other than just the MAC address of an endpoint. Network information includes site information, network device IP address, network device port, first authorized timestamp, last authorized timestamp, and the duration for which the endpoint has been available in the network. You can choose to distinguish the entries by the MAC address as done traditionally, or by using both the MAC address and the network information provided. If you choose to distinguish by MAC address and connectivity (network information), a selection is made automatically to detect the spoofed endpoint. You can either go with the automatic selection or choose the one you feel is the spoofed endpoint, and apply the appropriate remediation action for that endpoint. The remediation actions available are the Adaptive Network Control (ANC) policies configured in Cisco ISE.

Because this is the granular way of applying the policy, you won't see a listing for this policy in **Operations > Adaptive Network Control > Endpoint Assignment**.

For endpoints without concurrent MAC address detection and only NAT mode detection, an ANC policy is applied as described in [View and Manage Trust Scores for Endpoints, on page 655](#). In such a scenario, the endpoint gets listed under **Endpoint Assignment** in Cisco ISE.

For endpoints with both concurrent MAC addresses and NAT mode detection, the precedence is given to granular policy control. So, when you click **Apply ANC Policy**, you get the new **Apply ANC Policy** window with two options, to distinguish the entries.

You can also choose to change the ANC policy for an endpoint at any point of time. While changing the ANC policy, you have an option to choose more than one entry for which the ANC policy can be applied.



Note If you chose **Shutdown** as the remediation action, and you want to change the action, the endpoint won't be brought back automatically after changing the action. You must manually turn on the interface in the switch to which the endpoint is connected.

An ANC policy can also be removed at any point of time.

Before you begin

The dynamic author must be configured in the network devices. We recommend that you provision the network devices with the AAA configuration from Cisco DNA Center.

-
- Step 1** From the Cisco DNA Center GUI, choose **Policy > AI Endpoint Analytics > Endpoint Inventory > View endpoints in trust score view**.
- Step 2** Click the endpoint that you want to check and apply the ANC policy to.
- Step 3** Choose **Trust Score > Concurrent MAC Address**.
- Step 4** Click **Apply ANC Policy**.
- Step 5** In the **Apply ANC Policy** window, choose **Based on MAC address** or **Based on MAC address and connectivity**.
- Step 6** Choose the appropriate remediation action from the **Apply ANC Policy** drop-down list.
- Step 7** Click **Apply ANC Policy**.

After completing this task, when you return to the **Trust Score** view for that endpoint, you can see the ANC policy name and the network device IP address to which the policy was applied, along with the time at which the ANC policy was applied.

To verify the configuration, in the Cisco ISE GUI, choose **Operation > RADIUS > Live logs**. You can filter the **Identity** column by endpoint MAC address.

An entry for the CoA action that was initiated from Cisco ISE for this endpoint is listed. If you check the details, the **CoA Reason** shows the ANC policy that was applied by you for the endpoint.

Profiling Rules

Profiling rules in Cisco AI Endpoint Analytics enable you to group endpoints with a combination of common attributes. These attributes allow endpoint identification by Endpoint Type, OS Type, Hardware model, and Hardware Manufacturer. The profiling rules help you administer and manage many endpoints with ease.

Cisco AI Endpoints Analytics receives profiling data from network devices through DPI, media protocols, medical industry protocols, and more. Profiling data from Cisco ISE is communicated through pxGrid. These profiling attributes are then available in the device dictionary for authoring profile rules.

You can view the profiling rules in the **Profiling Rules** tab of Cisco AI Endpoints Analytics. In the table that is displayed under this tab, click a **Rule Name** entry to view the assigned profiles and attributes used.

The profiling rules that are used to profile the endpoints in Cisco AI Endpoint Analytics are:

- System Rules

- Custom Rules
- Cisco AI Rules

Rule Prioritization

The profiling rules in Cisco AI Endpoint Analytics have an order of priority. Profiling rule execution follows this rule priority to profile endpoints with high fidelity.

As user inputs are primary in Cisco AI Endpoint Analytics, the priority of the profiling rules is as follows:

- Administrator-created static profiles, for example, profiles added using the **Register Endpoints** option.
- Administrator-created custom rules.
- Cisco-provided system rules that are available by default.
- Auto-generated rules through the machine learning-enabled Smart Grouping workflow.

To view the set rule priority, click **Rule Prioritization** in the **Profiling Rules** window.

A registered endpoint can be profiled by multiple Cisco AI Endpoint Analytics rules for different profiling labels. The following table shows the design of profiling rules for two endpoints.

Endpoint 1	Endpoint 2
Hardware Model profiled by System Rule	Hardware Model profiled by System Rule
OS Type profiled by Cisco AI Rule	Hardware Model profiled by Custom Rule
Hardware Manufacturer profiled by Custom Rule	Hardware Model profiled by Cisco AI Rule

For Endpoint 2, rule priority results in the precedence of the custom rule over the others. The Hardware Model label for Endpoint 2 is profiled by the custom rule.

For Endpoint 1, different rules define different profile labels, and each label is profiled accordingly.

Filter Profiling Rules

-
- Step 1** In the **Profiling Rules** window, click **Filter**.
 - Step 2** Enter a name in the **Rule Name** field.
 - Step 3** Select values for endpoint attributes from the corresponding drop-down lists, to filter for a set of endpoints.
 - Step 4** Click **Apply**.
-

View Updated Profiling Rules

-
- Step 1** Go to the **Endpoint Inventory** window.
 - Step 2** Click the check box adjacent to the MAC Address of the endpoint to view the profiling details of the endpoint.

- Step 3** Click the information icon next to profile labels, and click the rule name to view the assigned profile and attributes details.
-

System Rules

Cisco AI Endpoint Analytics provides predefined rules called System rules for profiling endpoints. When Cisco AI Endpoint Analytics is deployed, it provides day zero visibility into endpoints without any need to configure specific rules.

Newly onboarded endpoints are profiled using system rules by default.

Network devices are managed in Cisco DNA Center in the **Provision > Network Devices > Inventory** window.

These network devices are profiled by the system rules and are not visible in the Cisco AI Endpoint Analytics **Endpoint Inventory** window. However, you can view the endpoints profiled by custom rules because the custom rules are created with network device as **Device Type**.

Automatic System Rule Updates for Endpoint Profiling

The system rules that are used for endpoint profiling in Cisco AI Endpoint Analytics are regularly updated to enhance profiling accuracy. Schedule automatic updates to receive updates in endpoint profiling system rules from Cisco. Your Cisco DNA Center receives updates at the configured time, and the changes are applied in Cisco AI Endpoint Analytics. In the **Profiling Rules** window (**Policy > AI Endpoint Analytics > Profiling Rules**), review the details of the changes in endpoint profiles, and accept or decline the system rule update.

If an endpoint's hardware model value changes due to an accepted system rule update, when you view the endpoint's details in the **Endpoint Inventory** tab, the **Hardware Model** field contains the name of the system rule update.

Before you begin

Configure and enable NBAR Cloud. See [Configure the NBAR Cloud Connector, on page 526](#).

To check the status of NBAR Cloud, choose **Policy > AI Endpoint Analytics > Overview**, and click **Configuration**.

-
- Step 1** From the main menu, choose **System > Settings > Cisco Accounts > Profile Rule Settings**.
The **Enabled** toggle button in the **Schedule Automatic Updates** area is set to active by default.
- Step 2** Click the buttons for the days of the week on which you want to schedule updates. You can choose multiple days. Then, use the **Time Slot** text fields to select the time for the update. It takes 30 minutes for the updates to be received by Cisco DNA Center. The second time slot area is not editable and displays the time when the scheduled update is expected to complete.
- Step 3** When your Cisco DNA Center receives a system rule update, a notification is displayed in the **Profiling Rules** window (**Policy > AI Endpoint Analytics > Profiling Rules**). The following notification is displayed when you click **Expand** in the dialog box:
- You are updated to the latest version *Name of Latest Version* and a recent Cisco profiling rule has changed the profiles of some endpoints. Review Update.
- Click **Review Update**

- Step 4** The **Endpoint Profile Update Review** dialog box is displayed. The dialog box contains information on the current stable update applied, the latest update received, and more. It also contains the following sections that you can click to view the related endpoint profile updates:
- a. **Major Updates:** Lists the endpoints whose profiles have had major changes, such as a Windows endpoint that is now recorded as a Linux endpoint.
 - b. **Minor Updates:** Lists the endpoints whose profiles have had minor changes, such as an updated version of Windows OS.
 - c. **Newly Profiled:** Lists the endpoints that were unprofiled previously and have now been assigned profile information.
- Step 5** After you review the endpoint profile changes, to accept the profile update, click **Mark As Approved Version** in the **Endpoint Profile Update Review** dialog box. If you do not agree with the endpoint profile changes, click **Rollback**. When you choose rollback, you must choose if you want to roll back to the last running version, or the last approved version, by clicking the corresponding option.
- You can also perform the accept and rollback actions from the **AI Endpoint Analytics > Overview > Configuration** window.
- Step 6** Click **X** to close the dialog box.

Custom Rules

In addition to the system rules, you can also create custom rules for profiling endpoints using a combination of endpoint attributes. Custom rules precede all the other endpoint profiling rules in Cisco AI Endpoint Analytics.

Logic and Conditions for Profiling Rules

You can create custom profiling rules in the **Endpoint Inventory** window. To create a custom profiling rule, you must create a logical condition based on endpoint attributes and values. These attributes are collected from network probe data and are different from the classification attributes available in the **Attribute Glossary** window.

A value is a user input that uniquely identifies the group of endpoints. The attributes and values create a regular expression with the help of the following operators.

Operators	Description
Contains	Attribute has the selected value.
Equals	Attribute is strictly mapped to the selected value.
Matches	Attribute should match the regular expression pattern of the selected value.
Starts With	Attribute should start with the selected value.



Note Contains, Equals, and Starts With are case-sensitive operators. For case-insensitive values, use the Matches operator.

These conditions can be further combined with the help of logic (**AND** and **OR**) to create a nested rule.

Create and Edit a Logical Condition

Follow the below instruction to create a logical condition.

-
- Step 1** In the **Choose Attribute Conditions** window, check the check box adjacent to the **Attribute** that you want to update.
- Step 2** Choose a option from the **Operator** drop-down lists.
- Step 3** Enter the value in the **Value** field.
- Step 4** Click **Next**.
- Step 5** In the **Add Logic to Conditions** window that is displayed, drag and drop the **AND** logic or the **OR** logic between the conditions in order to create a logical sequence of conditions for a custom rule.
- Note** You can also add or edit an attribute condition in the **Add Logical Conditions** window using the vertical ellipsis next to a condition.
- Step 6** Click **Next**.
-

Create a Custom Rule

-
- Step 1** In the **Endpoint Inventory** window, check the check box adjacent to the MAC address of the endpoints that you want to profile.
- Step 2** Click **Actions** and choose **Profile with Custom Rules**.
- Step 3** In the **Name Rule and Type** window that is displayed, in the **Rule Name** field, enter a name for the rule, and from the **Profile Label** drop-down list, choose a label.
- Depending on what you choose from the **Profile Label** drop-down list, a corresponding field, whose name is dynamically updated, is displayed. For example, if you choose **Endpoint Type**, the **Endpoint Type** field appears.
- Step 4** Enter a value in the new field that is displayed. As you start entering information, matching options are displayed. If an option matches your requirements, select the same. Otherwise, enter the complete type name.
- Step 5** Click **Next**.
- Step 6** In the **Choose Attribute Conditions** window that is displayed, create a logical condition.
- For more information, see [Logic and Conditions for Profiling Rules](#).
- Step 7** In the **Review Rule** window, review the list of endpoints that are going to be profiled with this custom rule.
- Step 8** Click **Next**.
- Step 9** Click **Profile**.
-

Edit a Custom Rule

-
- Step 1** In the **Profiling Rules** window, check the check box adjacent to the admin rule you want to edit.
- Step 2** Click **Actions** and select **Edit**.

- Step 3** In the **Edit** window that is displayed, in the **Rule Name** field, enter a name for the rule, and select or enter the profile details based on the **Profile Label** selected during the rule creation.
- Step 4** In the **Logic and Conditions** section, click on the vertical ellipsis and select **Edit** to update the logic and conditions for profiling rules. For more information, see [Logic and Conditions for Profiling Rules](#).
- Step 5** Click **Next**.
- Step 6** Click **Apply**.
After the existing rule is updated with new profiling details, the endpoints profiled with this rule are updated with new profiling details.

Delete a Custom Rule

- Step 1** In the **Profiling Rules** window, check the check box next to the rule that you want to delete.
- Step 2** Click **Actions** and choose **Delete**.
The following message is displayed:
`Do you really want to delete the selected Rule(s)?`
- Step 3** Click **Yes** to permanently delete the rule from Cisco AI Endpoint Analytics.
After the custom rule is deleted, the endpoints profiled with this rule are updated with system rules.

Export and Import Custom Profiling Rules Across Deployments Using APIs

Cisco DNA Center contains Cisco AI Endpoint Analytics APIs through which you can import, export, edit, and delete custom profiling rules.

To enable the Cisco AI Endpoint Analytics API bundle:

1. Click the menu icon (☰) and choose **Platform > Manage > Bundles**.
2. Find the bundle named **AI Endpoint Analytics** and click **Enable**.
3. The value in the **Status** column changes from **Disabled** to **Active**, and the list of APIs is displayed. You can also view the expected request and response payloads for each API.
4. After you enable the API bundle, the Cisco AI Endpoint Analytics APIs are added to the Cisco DNA Center Developer Toolkit. You can then access the APIs from the **Developer Toolkit** window (**Platform > Developer Toolkit**).

From both the **Bundles** and **Developer Toolkit** windows, you can:

- Generate code preview to view the API code that you can use in a different tool to run the API.
- Click **Try It** to run the API from the Cisco DNA Center GUI. You will receive a JSON response that you can copy and paste into a text editor of your choice to continue working with.

Cisco AI Rules for Smart Grouping

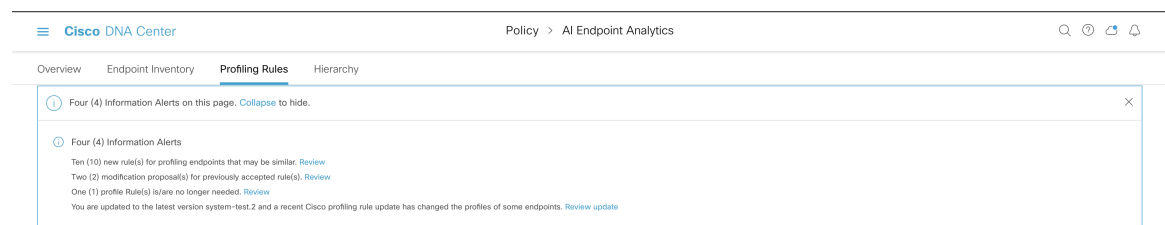
The Cisco AI Endpoint Analytics' AI algorithm analyzes data about endpoint profiling labels and groups across deployments and provides you with smart profiling rules suggestions.

The **AI Proposal** dashlet in the Cisco AI Endpoint Analytics **Overview** tab displays the following rule suggestions based on the learnings from endpoint clusters:

- New profiling rules for unprofiled or unlabeled endpoints in your network. For more information, see [New Profiling Suggestions for Similar Endpoints in Your Network, on page 667](#)
- Modification suggestions for existing profiling rules in your network that are based on the endpoint profiling data changes that AI algorithm has learned across deployments. For more information, see [Smart Modification Suggestions for Your Endpoint Profiling Rules, on page 669](#).
- Deletion suggestions for profiling rule that contain an incorrect label that are based on the endpoint profiling data changes that AI algorithm has learned across deployments. When you accept a deletion rule, the incorrect profiling label is removed from the impacted endpoints. The profiling type value for the endpoints is then either empty or returns to a previously assigned label. For more information, see [Smart Suggestions to Delete Profiling Rules, on page 671](#).

You can also initiate the workflows to review and apply proposals for changes to endpoint profiling rules from the **Profiling Rules** tab of Cisco AI Endpoint Analytics. The **Profiling Rules** displays a dialog box with information alerts. In the information alert dialog box, click **Expand** to view the available proposals for changes to endpoint profiling rules. Click **Review** next to the information alert that you want to examine to initiate the corresponding workflow.

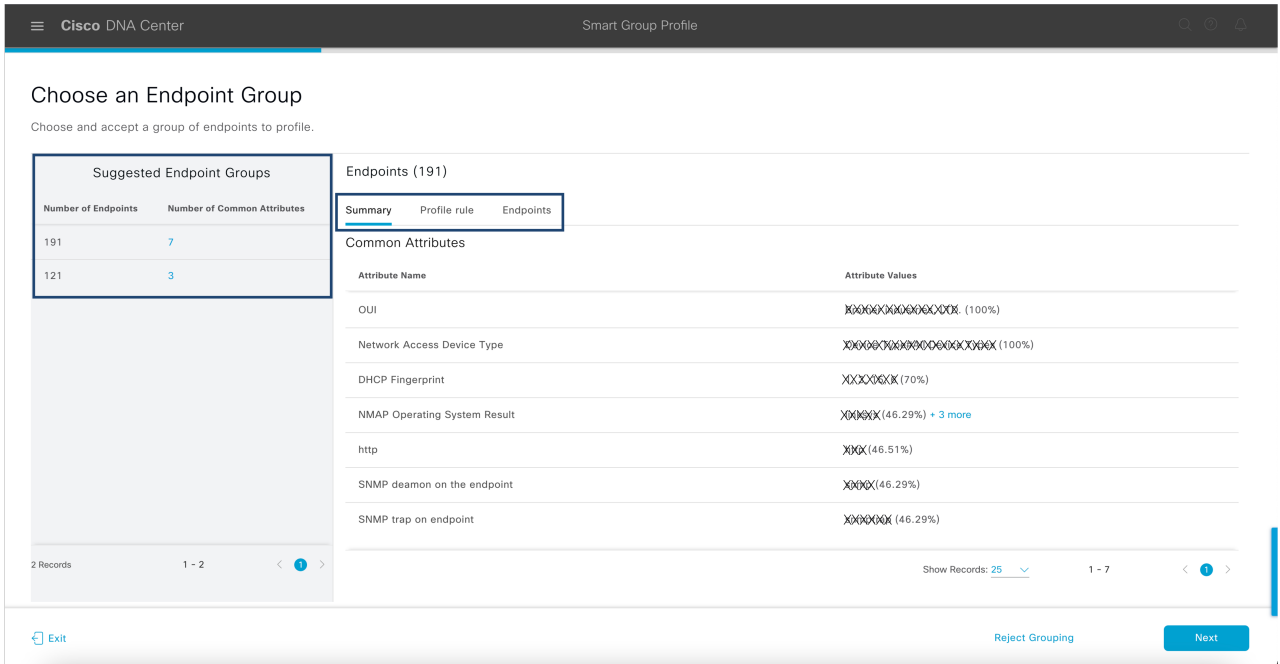
Figure 35: Information Alerts in the Profiling Rules Tab



New Profiling Suggestions for Similar Endpoints in Your Network

- Step 1** In the **AI Proposals** dashlet, click the **Review** button next to **New rule(s) for profiling endpoints that many be similar**. The **Smart Group Profile** workflow is launched.
- Step 2** The **Choose an Endpoint Group** window that is displayed contains a list of new profiling rules suggestions in the left pane. Click an entry in the list to view the details of the profiling rule in the right pane.

Figure 36: Choose an Endpoint Group Window of the Smart Group Profile Workflow

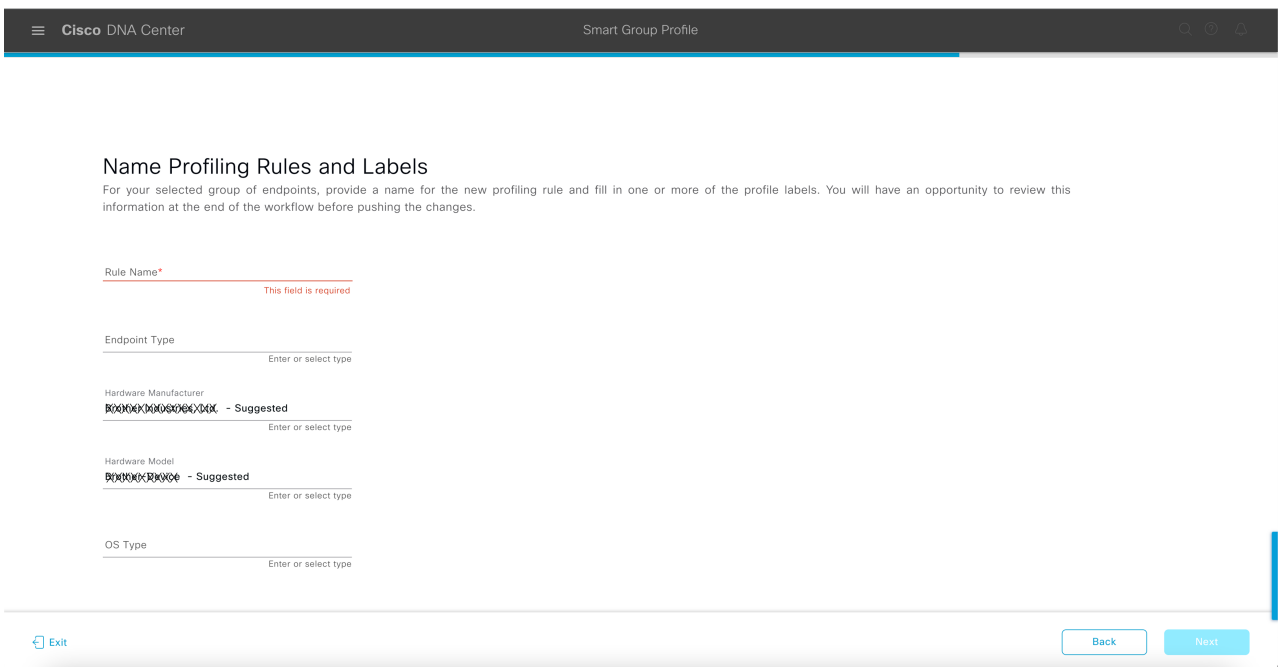


The right pane contains the **Summary**, **Profile Rule**, and **Endpoints** tabs that provide a quick view of the details of the profiling rule that is suggested.

Step 3 Click **Next** to create the suggested profiling rule.

Step 4 In the **Name Profiling Rules and Labels** window that is displayed, in the **Rule Name** field, enter a name for the rule.

Figure 37: Name Profiling Rules and Labels Window of the Smart Group Profile Workflow



Step 5 In one or more of the following fields, enter the required values. You must enter a value in at least of the fields to proceed to the next step.

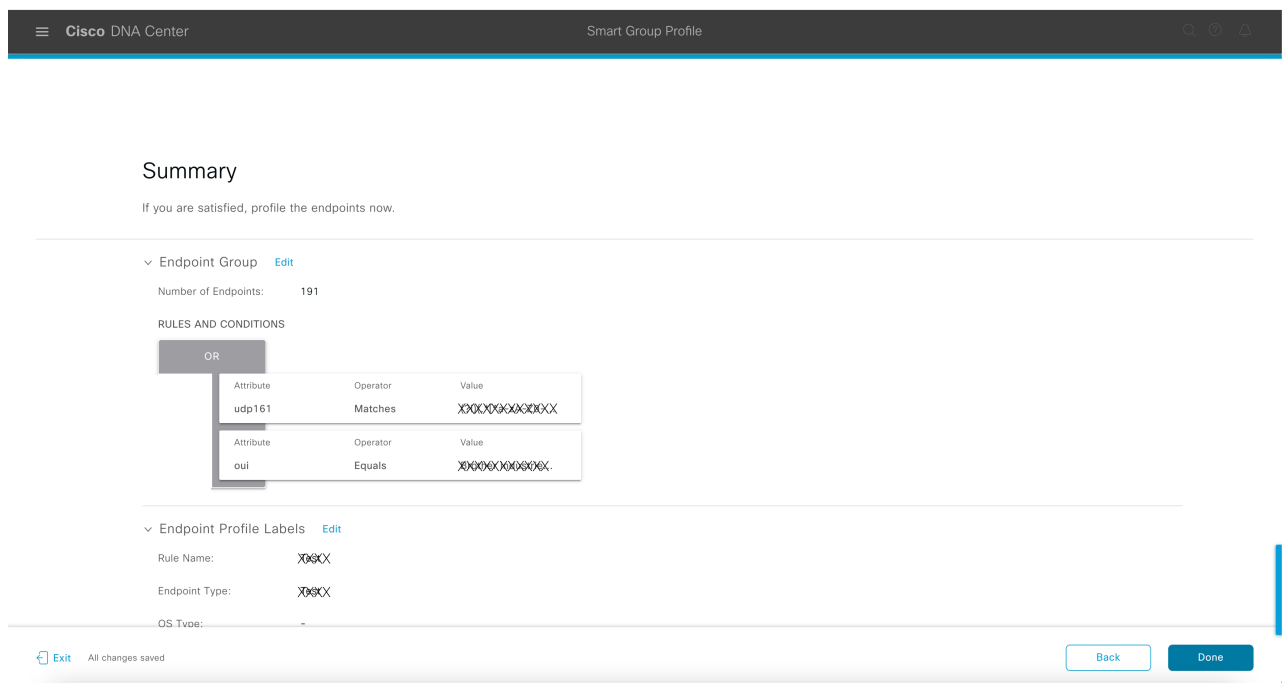
- **Endpoint Type**
- **Hardware Manufacturer**
- **Hardware Model**
- **OS Type**

If the AI algorithm identifies a profiling label for the endpoints, the label is displayed as a suggestion in the corresponding field. You can choose to proceed with the suggested label or select a different label.

Step 6 Click **Next** to continue.

Step 7 In the **Summary** window, review the details of profiling rule. To make any changes, click **Edit**.

Figure 38: Summary Window of the Smart Group Profile Workflow



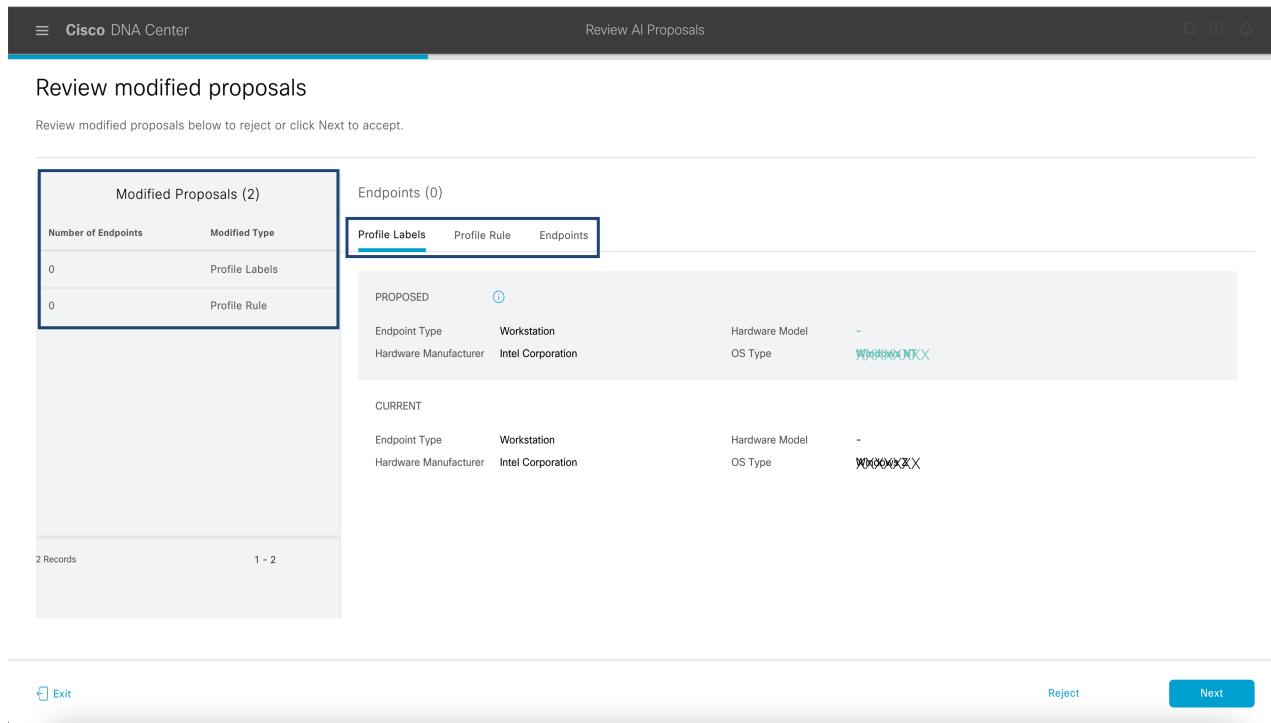
Step 8 To create the profiling rule, click **Done**.

Smart Modification Suggestions for Your Endpoint Profiling Rules

Step 1 In the **AI Proposals** dashlet, click the **Review** button next to **Modification proposal(s)** for previously accepted rule(s). The **Smart Group Profile** workflow is launched.

Step 2 The **Review modified proposals** window that is displayed contains a list of modification proposals for existing profiling rules. Click an entry in the list to view the details of the modification suggestion in the right pane.

Figure 39: Review Modified Proposals Window of the Review AI Proposals Workflow

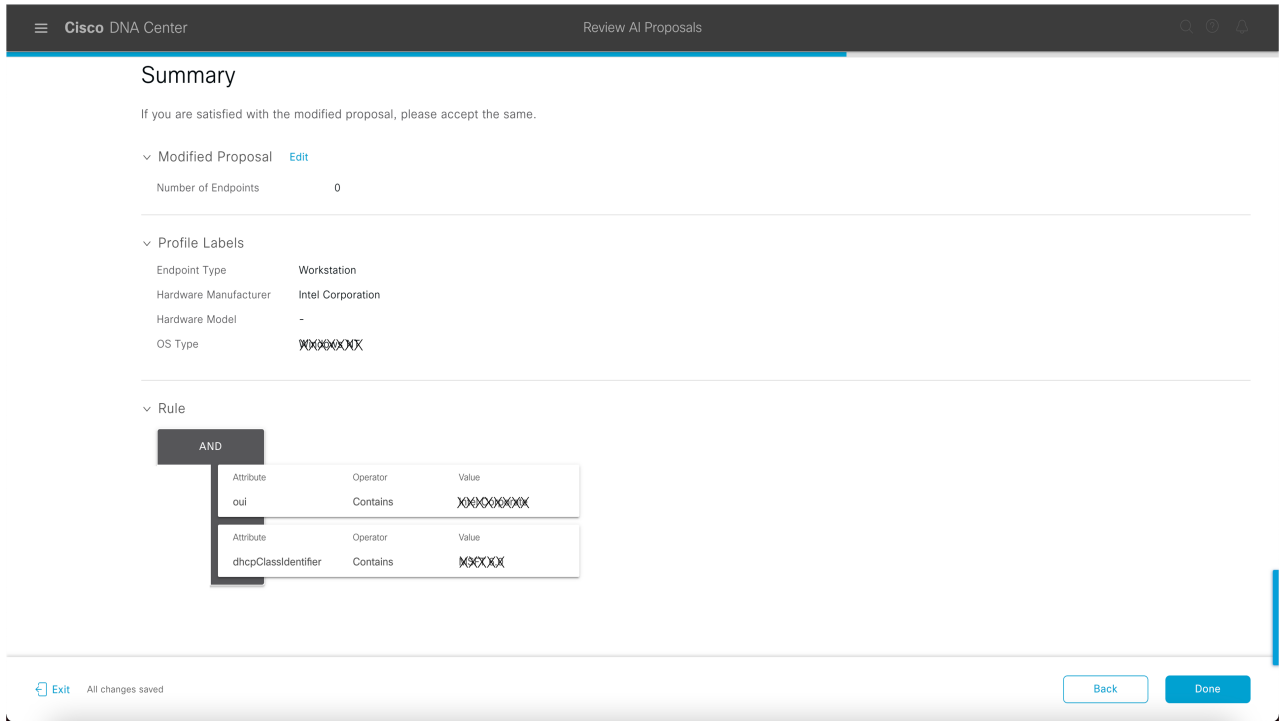


The right pane contains the **Profile Labels**, **Profile Rule**, and **Endpoints** tabs that provide a quick view of the details of the modified profiling rule that is suggested.

Step 3 Click **Next** to update the profiling rule as suggested.

Step 4 In the **Summary** window, review the details of profiling rule. To make any changes, click **Edit**.

Figure 40: Summary Window of the Review AI Proposals Workflow



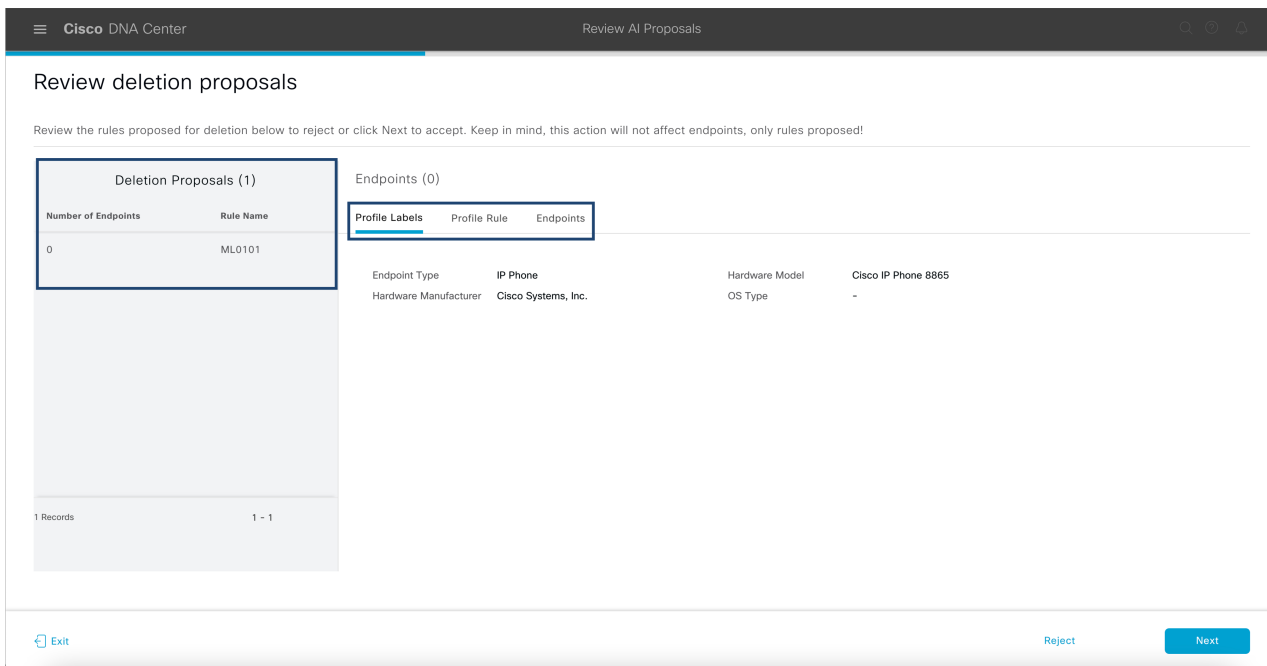
Step 5 To update the profiling rule, click **Done**.

Smart Suggestions to Delete Profiling Rules

Step 1 In the **AI Proposals** dashlet, click the **Review** button next to **Profiling Rules(s) is/are no longer needed**. The **Review AI Proposals** workflow is launched.

Step 2 The **Review deletion proposals** window that is displayed contains a list of deletion proposals for existing profiling rules. Click an entry in the list to view the details of the deletion suggestion in the right pane.

Figure 41: Review Deletion Proposals Window of the Review AI Proposals Workflow

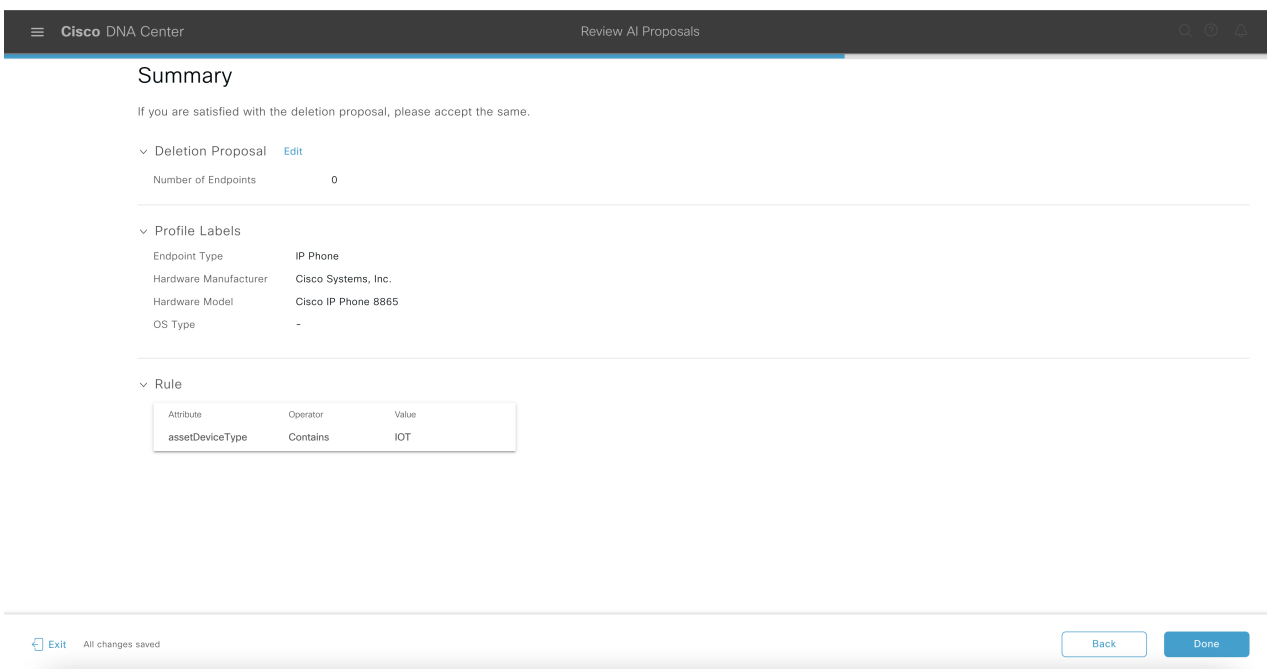


The right pane contains the **Profile Labels**, **Profile Rule**, and **Endpoints** tabs that provide a quick view of the details of the modified profiling rule that is suggested.

Step 3 Click **Next** to update the profiling rule as suggested.

Step 4 In the **Summary** window, review the details of profiling rule. To make any changes, click **Edit**.

Figure 42: Summary Window of the Review AI Proposals Workflow



Step 5 Click **Done** to accept the deletion proposal.

Import Profiling Rules

You can migrate your custom profiling rules and Cisco AI rules by importing the .json files.

- Step 1** In the **Profiling Rule** window, click **Actions**
- Step 2** Choose **Import Profiling Rules**.
- Step 3** Click **Choose a file** and browse to the .json file in your system.
- Step 4** Click **Ok**.
-

Export Profiling Rules

You can export and back up custom rules and Cisco AI profiling rules from Cisco AI Endpoint Analytics. The **Export Profiling Rules** option exports all the available custom rules and Cisco AI profiling rules. You cannot selectively export rules.

- Step 1** In the **Profiling Rules** window, click **Actions**.
- Step 2** Choose **Export Profiling Rules**.
- Step 3** Click **Yes** to export all the custom and ML profiling rules. Click **No** to exit.
- Note** You can import the same file again into Cisco AI Endpoint Analytics.
-

Hierarchy

Cisco AI Endpoint Analytics hierarchy helps you create logical groupings of endpoints, based on the endpoint types. Creating categories and subcategories for the endpoints focuses on endpoint visibility and simplifies the authorization process.

You can create categories from the **All Endpoints** default parent category. The category details such as total number of endpoints, endpoint types, and subcategories are listed within individual boxes in the **Hierarchy** window.

You can create, edit, and delete the categories to reorder the hierarchy.

Create Category and Subcategory

- Step 1** In the **Hierarchy** window, click the horizontal ellipsis of the parent category.
- Step 2** Click **Create Category**.

Step 3 Enter a category name.

Step 4 Click **Enter**.

What to do next

After you create a category, you can drag and drop endpoint types from the **Endpoint Type** window, or edit the category to add endpoints to it.

Edit a Category or Subcategory

Step 1 In the **Hierarchy** window, click on the horizontal ellipsis of the category.

Step 2 Click **Edit**.

Step 3 In the **Edit** window that is displayed, enter the **Category Name**.

Step 4 Enter the **Parent Category** from the drop-down menu, if you want to reassign the category.

Step 5 Click the **Endpoint Type** tab.

Step 6 Click **Actions** and select **Add Endpoint Type**.

Step 7 Choose the endpoint type from the **Search Dropdown** list.

Step 8 Click **Save**.

What to do next

In the Endpoint Type window, you can filter the endpoint types as **All**, **Available**, and **Assigned**.

Delete Endpoint Types from Category

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the category that you want to delete.

Step 2 Click **Edit**.

Step 3 In the **Edit** window, click the **Endpoint Type** tab.

Step 4 Check the check box adjacent to the endpoint type that you want to delete.

Step 5 Click **Actions** and choose **Remove From Category**.

The following message displays:

Are you sure you want to delete this category?

Step 6 Click **Yes** to delete the endpoint from the category. Click **No** to exit.

Reassign Endpoint Types from Category

Step 1 In the **Hierarchy** window, click the horizontal ellipsis of the category.

- Step 2** Click **Edit**.
- Step 3** In the **Edit** window, click the **Endpoint Type** tab.
- Step 4** Check the check box adjacent to the endpoint type that you want to reassign.
- Step 5** Click **Actions** and choose **Re-assign to existing category** or **Re-assign to a new category**.

Option	Steps
Re-assign to existing category	<ul style="list-style-type: none"> a. In the Reassign window, choose an existing category from the Category drop down list. b. Click Save.
Re-assign to a new category	<ul style="list-style-type: none"> a. In the Reassign window, choose New Category from the Category drop down list. b. Choose a parent category from the Parent Category drop down list. c. Enter the category name in the New Category field. d. Click Save.

Delete a Category

Before you begin

Before you delete a parent category, check its subcategories. You can reassign the subcategories to another existing category or to a new category. Otherwise, all the subcategories are deleted along with the parent category. You can also reassign the subcategories while you are deleting a category.

- Step 1** In the **Hierarchy** window, click the horizontal ellipsis of the category.
- Step 2** Click **Delete**.

If you are deleting a category that has subcategories assigned to it, the **Reassign Relationships** dialog box is displayed. Choose one of the following options:

Option	Condition	Steps
Reassign to an existing category	Reassign the subcategories to an existing category.	<ul style="list-style-type: none"> a. Select a category from the Category drop-down list. b. Click Reassign. <p>The parent category is deleted and its subcategories will be reassigned to the selected category.</p>

Option	Condition	Steps
Reassign to a new category	Reassign the subcategories to an existing category.	<ol style="list-style-type: none"> <li data-bbox="1073 285 1481 348">a. Select a category from the Parent Category drop-down list. <li data-bbox="1073 369 1481 432">b. Enter the category name in the New Category field. <li data-bbox="1073 453 1481 485">c. Click Reassign. <p data-bbox="1073 516 1481 615">The parent category is deleted and its subcategories are reassigned to the new category.</p>
Remove from category	Delete the subcategories along with the parent category.	<p data-bbox="1073 636 1481 667">Click Reassign.</p> <p data-bbox="1073 688 1481 751">The parent category and its subcategories are deleted.</p>



CHAPTER 28

Troubleshoot Network Devices Using Network Reasoner

- [Network Reasoner Overview, on page 677](#)
- [Validate Cisco SD-Access Migration Using the MRE Workflow, on page 677](#)
- [Troubleshoot High CPU Utilization, on page 679](#)
- [Troubleshoot a Power Supply Failure, on page 680](#)
- [Troubleshoot a Downed Interface, on page 681](#)
- [Troubleshoot Network Connectivity, on page 682](#)
- [Troubleshoot IP Connectivity of a Device, on page 683](#)
- [Troubleshoot Wireless Clients Using the MRE Workflow, on page 683](#)
- [Troubleshoot Wireless APs Using the MRE Workflow, on page 684](#)
- [Troubleshoot Unmonitored Devices Using the MRE Workflow, on page 685](#)
- [Scan the Network for Bugs, on page 686](#)
- [Scan Cisco DNA Center for Bugs, on page 689](#)

Network Reasoner Overview

The Network Reasoner tool allows you to troubleshoot various issues on your network quickly. Click the menu icon (☰) and choose **Tools > Network Reasoner** to launch the Network Reasoner dashboard. The Network Reasoner dashboard hosts separate workflows that you can use to proactively troubleshoot network issues. The dashboard provides a brief description of the workflows, the number of affected devices in the last 24 hours, and the impact of running a workflow on a network.



Note You must install the Machine Reasoning package to view the Network Reasoner feature under the **Tools** menu. For more information, see the [Cisco DNA Center Administrator Guide](#).

Validate Cisco SD-Access Migration Using the MRE Workflow

The following Machine Reasoning Engine (MRE) workflows assist in planning your migration to Cisco SD-Access:

- SDA Hardware Readiness Check
- SDA Software Readiness Check
- Redundant Link Check
- L3 Access Check
- MTU Link Check
- SDA Health Check
- SDA Scale Limits Check

Step 1 Click the menu icon (☰) and choose **Tools > Network Reasoner**.

Step 2 In the **Network Reasoner** dashboard, click the following workflows as required:

Workflow	Description	Action
SDA Hardware Readiness Check	Checks whether the hardware is ready for Cisco SD-Access migration.	<ol style="list-style-type: none"> a. Click SDA Hardware Readiness Check. b. Click Run Machine Reasoning.
SDA Software Readiness Check	Checks whether the software is ready for Cisco SD-Access migration.	<ol style="list-style-type: none"> a. Click SDA Software Readiness Check. b. Click Run Machine Reasoning.
Redundant Link Check	Checks whether any redundant uplinks are present in your device and if there are ways to increase availability by configuring redundant uplinks on the access switches.	<ol style="list-style-type: none"> a. Click Redundant Link Check. b. Select an appropriate device. c. Click Troubleshoot.
L3 Access Check	Checks whether your network has access switches that are running Layer 3 routing protocols to move to Cisco SD-Access with minimal design changes.	<ol style="list-style-type: none"> a. Click L3 Access Check. b. Select an appropriate device. c. Click Troubleshoot.
MTU Link Check	Checks whether the links between the main network devices and the access, core, and other switches are configured with the correct MTU.	<ol style="list-style-type: none"> a. Click MTU Link Check. b. Select an appropriate device. c. Click Troubleshoot.
SDA Health Check: Fabric Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing fabrics.	<ol style="list-style-type: none"> a. Click Fabric Count. b. Click Run Machine Reasoning.

Workflow	Description	Action
SDA Health Check: SDA Scale Limits Check	Checks whether the number of client endpoints, network devices, and configured fabrics in Cisco DNA Center are within the published SDA limits.	<p>a. Click SDA Scale Limits Check.</p> <p>b. Click Run Machine Reasoning.</p>
SDA Health Check: Client Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing clients.	<p>a. Click Client Count.</p> <p>b. Click Run Machine Reasoning.</p>
SDA Health Check: Device Count	Checks the health of the Cisco DNA Center cluster to determine whether it is reaching any scale limit thresholds due to managing network devices.	<p>a. Click Device Count.</p> <p>b. Click Run Machine Reasoning.</p>

Troubleshoot High CPU Utilization

CPU utilization troubleshooting support is available only for the following network devices with software version 16.9.3 and later:

- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

Step 1 Click the menu icon (☰) and choose **Tools > Network Reasoner**.

Step 2 Click the **CPU Utilization** tab.

The **CPU Utilization** window displays the filtered list of devices with high CPU utilization in the past 24 hours.

Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag, Device Name, IP Address, Device Type, Site, or Reachability**.

Step 4 Click **Troubleshoot**.

Step 5 In the **Reasoner Input** window, enter the **CPU Utilization Threshold** percentage that you want to check against.

Step 6 Click **Run Machine Reasoning**.

Note The following processes, if observed, are considered for detailed analysis:

- **MATM Process Group:** MATM RP Shim, NGWC Learning, and VMATM Callback
- **IOSXE Process Group:** IP Input, ARP Input, IOSXE-RP Punt Se, SISF Main Thread, DAI Packet, and ARP Snoop

In the **CPU Utilization** window, you can see the **Root Cause Analysis** of the high CPU utilization for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 7 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 8 Click the **Conclusion** tab to see the processes that consume more CPU and the utilization percentage.

Step 9 Click **View Relevant Activities** for each process to view the **Activity Details** in the right pane.

Step 10 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Note The Machine Reasoning Engine (MRE) implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

Troubleshoot a Power Supply Failure

Power supply troubleshooting workflow support is available only for the following network devices with software version 16.6.1 and later:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

Step 1 Click the menu icon (☰) and choose **Tools > Network Reasoner**.

Step 2 Click the **Power Supply** tab.

The **Power Supply** window displays the filtered list of devices with power supply failures in the past 24 hours.

Click **All** to see the list of all devices in the inventory. You can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and filter the devices by entering **Tag**, **Device Name**, **IP Address**, **Device Type**, **Site**, or **Reachability**.

Step 4 Click **Troubleshoot**.

In the **Power Supply** window, you can see the **Root Cause Analysis** of the power supply failure for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 5 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 6 Click the **Conclusion** tab to see the **Stack Identifier**, **Product ID**, **Serial Number**, and **Status** of the power supply for the chosen device and the suggested action.

Step 7 Click **View Relevant Activities** for each stack identifier to view the **Activity Details** in the right pane.

Step 8 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Note The Machine Reasoning Engine (MRE) implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.


Troubleshoot a Downed Interface

Interface down troubleshooting workflow support is available only for the following network devices with software version 16.9.3, and later:

- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

Step 1 Click the menu icon () and choose **Tools > Network Reasoner**.

Step 2 Click the **Interface Down** tab.

The **Interface Down** window displays the filtered list of devices with an interface that went down in the past 24 hours. Click **All** to see the list of all devices from the inventory, and you can choose any device to run the workflow.

Step 3 Choose the device that you want to troubleshoot.

Click **Filter** and enter the devices by entering **Tag, Device Name, IP Address, Device Type, Site, or Reachability**.

Step 4 Click **Troubleshoot**.

Step 5 In the **Reasoner Input** window, enter the interface name that you suspect has issues.

Step 6 Click **Run Machine Reasoning**.

In the **Interface Down** window, you can see the **Root Cause Analysis** of the downed interface for the chosen device.

The **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.

Step 7 (Optional) Click **Stop** to stop the ongoing reasoning activity.

Step 8 Click the **Conclusion** tab to see the potential root causes for the interface down issue and the suggested action.

Step 9 Click **View Relevant Activities** for each root cause analysis to view the **Activity Details** in the right pane.

Step 10 (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.

Note The Machine Reasoning Engine (MRE) implements a system-terminate algorithm that detects and terminates network reasoner workflows when thresholds exceed a specified level, or when no events are received from the timeout request for inactivity.

Troubleshoot Network Connectivity

Only the following network devices running Cisco IOS-XE software version 16.9.3 or later support the network connectivity troubleshooting:

- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9600 Series Switches

Use the following procedure to check the reachability of an endpoint from a device using IP address:

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** Click the **Network Connectivity** tab.
- Step 3** You can view the device table with details, such as **Device Name**, **IP Address**, **Device Type**, **Site**, **Reachability**, **Role**, and **Platform**.
- Step 4** Select a device and click **Troubleshoot**.
- Step 5** In the **Destination IP address** field of the **Reasoner Inputs** window, enter a valid IP address and click **Run Machine Reasoning**.
- Note** Provide the Virtual Routing and Forwarding (VRF) name, if applicable.
- Step 6** In the **Root Cause Analysis** window, under **Reasoning Activity**, you can view various workflows that are validated as a part of the troubleshooting process.
- Step 7** In the **Conclusions** tab, you can view the status of the validation check and the suggested action.
-

Troubleshoot IP Connectivity of a Device

As ping is a simple command, IP connectivity troubleshooting support is available for all the network devices.

Before you begin

- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Create a user role with write permissions for Machine Reasoning under the **System** function. For more information, see Configure Role-Based Access Control in the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** In the **Network Reasoner** dashboard, click **Ping Device**.
- Step 3** In the **Devices** window, choose a device and click **Troubleshoot**.
- Step 4** In the **Reasoner Inputs** window, enter **Target IP Address** and click **Run Machine Reasoning**.
- Step 5** Click **View Details** to view the ping status.
-

Troubleshoot Wireless Clients Using the MRE Workflow

Use this procedure to troubleshoot wireless client issues using the MRE workflow.

**Note**

- Wireless client troubleshooting workflow support is available only for network devices with Cisco IOS-XE software version 17.3.4 and later.
- The MRE workflow doesn't support HA, which means that if a switchover occurs during the workflow, you must repeat the workflow.

Before you begin

Make sure that the Machine Reasoning Engine (MRE) knowledge base is updated with the latest knowledge packs. For more information, see the "Update the Machine Reasoning Knowledge Base" topic in the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** Click the **Wireless Client Data Collection** tile.
The **Devices** window shows the filtered wireless controller devices.
- Step 3** Choose the wireless controller that you want to troubleshoot and click **Troubleshoot**.
- Step 4** In the **Reasoner Inputs** window, complete the following fields:
- **Troubleshoot Duration**
 - **Client MAC Address**
 - **PCAP Interface**: Click the drop-down arrow and choose an interface from the list. Use this option if packet capture is required.
- Step 5** Click **Run Machine Reasoning**.
The **Wireless Client Data Collection** slide-in pane is displayed.
- Step 6** In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process. Optionally, click **Stop** to stop the ongoing reasoning activity.
- Step 7** Wait for the troubleshooting process to complete. After it completes, you can view the troubleshooting files under the **Conclusions** tab.
- Step 8** (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.
- Step 9** (Optional) You can view the last troubleshooting files in the **Wireless Client Data Collection** slide-in pane when you start the Wireless Client troubleshooting workflow.
-

Troubleshoot Wireless APs Using the MRE Workflow

Use this procedure to troubleshoot wireless AP issues using the MRE workflow.

**Note**

- Wireless AP troubleshooting workflow support is available only for network devices with Cisco IOS-XE software version 17.3.4 and later.
- The MRE workflow doesn't support HA, which means that if a switchover occurs during the workflow, you must repeat the workflow.

Before you begin

Make sure that the MRE knowledge base is updated with the latest knowledge packs. For more information, see [Update the Machine Reasoning Knowledge Base in the *Cisco DNA Center Administrator Guide*](#).



-
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** Click the **Wireless AP Data Collection** tile.
- Step 3** The **Devices** window shows the filtered wireless controller devices. Choose the wireless controller device that you want to troubleshoot for the AP and click **Troubleshoot**.
- Step 4** In the **Reasoner Inputs** window, complete the following fields:
- **Troubleshoot Duration**
 - **Two AP MAC Address:** Enter the AP MAC address for Ethernet and radio.
 - If packet capture is required, use the following option:
 - **PCAP Interface:** Click the drop-down list to choose the interface.
 - **AP IP Address:** Enter the AP IP address.
 - **AP Name**
- Step 5** Click **Run Machine Reasoning**.
The **Wireless AP Data Collection** slide-in pane appears.
- Step 6** In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process. Optionally, click **Stop** to stop the ongoing reasoning activity.
- Step 7** Wait for the troubleshooting process to complete. After it completes, you can view the troubleshooting files under the **Conclusions** tab.
- Step 8** (Optional) Click **Run Again** to rerun the troubleshooting process for the same device.
- Step 9** (Optional) You can view the last troubleshooting files in the **Wireless AP Data Collection** slide-in pane when you start the Wireless AP troubleshooting workflow.
-

Troubleshoot Unmonitored Devices Using the MRE Workflow

Use this procedure to troubleshoot unmonitored devices or devices that are not showing Assurance data. The Troubleshooting Unmonitored Devices workflow supports only switches, Cisco AireOS Wireless Controllers, and Cisco Catalyst 9800 Series Wireless Controllers.

Before you begin

Make sure that the Machine Reasoning Engine (MRE) knowledge base is updated with the latest knowledge packs. For more information, see the "Update the Machine Reasoning Knowledge Base" topic in the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon () and choose **Tools > Network Reasoner**.
- Step 2** Click the **Assurance Telemetry Analysis** tile.
- Step 3** The **Devices** window shows the filtered unmonitored devices. Choose the device that you want to troubleshoot and click **Troubleshoot**.
- The **Assurance Telemetry Analysis** slide-in pane is displayed. In the **Root Cause Analysis** area, the **Reasoning Activity** tab shows the various parameters that are checked as part of the troubleshooting process.
- Step 4** Click **Stop** to stop the ongoing reasoning activity.
- After the troubleshooting is complete, the **Machine Reasoning Completed** dialog box is displayed.
- Step 5** Click **View Details**.
- Step 6** You can view the troubleshooting files under the **Conclusions** tab. The issue is highlighted with an icon () and the **Suggested Action** is displayed below the issue.
- You can troubleshoot the unmonitored device with the suggestions provided.
- Step 7** Click **Run Again** to rerun the troubleshooting process for the same device.
- Step 8** You can also troubleshoot the devices from the **Inventory** tab. Scroll down to view the **Health Score** column. Click **No Health** under the **Health Score** column and click **View Assurance Telemetry Analysis** to run the troubleshooting process.
-

Scan the Network for Bugs

The Cisco DNA Center network bug identifier tool allows you to scan the network for a selected set of defects or bugs that have been identified previously and are known to Cisco.

The Cisco DNA Center network bug identifier helps in identifying specific patterns in the device configuration or in the operational data of the device and matches them with known defects based on those patterns. This tool provides both bug-focused and device-focused views.

Cisco DNA Center collects network device configuration and operational data by running CLI commands on network devices, and then sends the information to the CX Cloud to be processed for exposure to potential security advisories or bugs. Cisco DNA Center invokes the following CLI commands for the network bug identifier tool:


- **show buffers summary**
- **show cef interfaces**
- **show clock**
- **show crypto eli all**
- **show crypto isakmp sa detail**

- **show eigrp service-family ipv4 neighbors**
- **show environment all**
- **show interfaces counters error**
- **show interfaces summary**
- **show inventory**
- **show ip interface brief**
- **show ip nat translations verbose**
- **show ip nbar protocol-discovery**
- **show ip nbar resources flow**
- **show ip nhrp**
- **show ip nhrp summary**
- **show ip route**
- **show ip ssh**
- **show ip vrf**
- **show logging**
- **show performance monitor cache detail**
- **show platform software route-map fp active map**
- **show pnp profile**
- **show redundancy**
- **show redundancy application group**
- **show running-config all**
- **show scp status**
- **show stackwise-virtual**
- **show startup-config**
- **show terminal**
- **show version**

The following procedure explains how to identify bugs using the network bug identifier tool.

Before you begin

- Install the Cisco DNA Center core package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).

- Step 1** Click the menu icon () and choose **Tools > Network Reasoner**.
- Step 2** Select **Network Bug Identifier**.
- Step 3** Click **Scan Network**.
- Step 4** In the **Scan Network** window, choose whether you want to scan your system for bugs **Now** or schedule it for **Later**.
The dashboard progress indicator shows the list of devices scanned in batches of 10. When the scan is done, the **Network Bug Identifier** window appears.
- Step 5** Use the top pane to view information about the results of the scan, rescan the network, and change scan settings, as follows:

Item	Description
Bug Summary	Number of Catastrophic , Severe , and Moderate bugs in your network.
Affected Devices	Number of the following device types that were scanned: <ul style="list-style-type: none"> • Routers • Switches and Hubs
Scan Mode	Method used to perform the scan: <ul style="list-style-type: none"> • Essential: Scan performed using the Cisco Network Reasoner Engine (NRE). • CX Cloud: Scan performed using the CX Cloud.
Re-scan Network	Click this button to scan your network again.
Settings	Click the Settings icon to do the following: <ul style="list-style-type: none"> • Enable or disable weekly scans. • Enable or disable the CX Cloud to scan your network.

- Step 6** Click the **Bugs on Devices** tab to view information about the bug, such as **Bug ID**, **Name**, **Affected Devices**, **Severity**, **Affected Versions**, and **Workaround**.
Click any hyperlinked value to display more information about it.
- Step 7** Click the **Devices** tab to view information about the devices, such as **Device Name**, **Image Version**, **IP Address**, **Device Type**, **Bugs**, **Scan Status**, **Scan Mode**, **Site**, and **Reachability**.
Click any hyperlinked value to display more information about it.
- Step 8** From the **Devices** tab, click **Tag Device** to create, edit, or delete tags on the devices.

Scan Cisco DNA Center for Bugs

The **System Bug Identifier** tool provides an option to identify bugs in the Cisco DNA Center. The following procedure explains how to enable the **System Bug Identifier** tool:

Before you begin

- Install the Cisco DNA Center core package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- Install the Machine Reasoning package. For more information, see Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Tools > Network Reasoner**.
- Step 2** Select **System Bug Identifier**.
- Step 3** Click **Scan System**.
- Step 4** In the **Scan System** window, choose whether you want to scan your system for bugs **Now** or schedule it for **Later**.
- Step 5** The **System Bug Identifier** window shows the **BUG SUMMARY** and the **Bugs Identified on Your System** table. In addition to basic bug information, this window shows information, such as when the bug was first and last identified, the frequency that it was identified and affected versions.
- Step 6** Click the **Bug ID**. The **Bug Details** dialog box displays the details of the bug.
- Step 7** Click the arrow next to **Bug ID** to go to the **Bug Search Tools** window, which shows more details about the bugs.
-



CHAPTER 29

Identify Network Security Advisories

- [Security Advisories Overview, on page 691](#)
- [Prerequisites, on page 691](#)
- [View Security Advisories, on page 692](#)
- [Schedule a Security Advisories Scan, on page 693](#)
- [Enable the Try Cisco CX Cloud Success Track to Identify Security Advisories, on page 694](#)
- [CLI Commands Invoked for Security Advisories, on page 695](#)
- [Rescan the Network to Identify Security Advisories, on page 695](#)
- [Hide and Unhide Devices from an Advisory, on page 696](#)
- [Hide and Unhide Advisories from a Device, on page 696](#)
- [Add Notification for a New Security Advisory KB, on page 697](#)
- [View Security Advisories in the Inventory, on page 698](#)
- [Add a Match Pattern, on page 698](#)
- [Define AND/OR for the Match Pattern, on page 699](#)
- [Edit the Match Pattern, on page 699](#)
- [Delete the Match Pattern, on page 700](#)

Security Advisories Overview

The Cisco Product Security Incident Response Team (PSIRT) responds to Cisco product security incidents, regulates the Security Vulnerability Policy, and recommends [Cisco Security Advisories and Alerts](#).

The Security Advisories tool uses these recommended advisories, scans the inventory within Cisco DNA Center, and finds the devices with known vulnerabilities.

Prerequisites

To use the Security Advisories tool, you must install the Machine Reasoning package. See *Download and Install Packages and Updates* in the [Cisco DNA Center Administrator Guide](#).

If you log in to Cisco DNA Center as an Observer, you cannot view the **Security Advisories** tool in the home page.

View Security Advisories

Step 1 Click the menu icon (☰) and choose **Tools > Security Advisories**.

Step 2 If you are launching the **Security Advisories** window for the first time, click **Scan Network**.

Cisco DNA Center uses the knowledge base to identify security issues and improve automated analysis. We recommend that you update the knowledge base on a regular basis to view the latest security advisories.

- a) Click the menu icon (☰) and choose **System > Settings > Machine Reasoning Engine**.
- b) Either click **Import** or click **Download Latest** to download the latest available knowledge base. After the download, click **Import**.
- c) Click the **AUTO UPDATE** toggle button to subscribe to automatic updates.

Step 3 The **ADVISORIES** area displays the distribution percentage of impact on the network, such as **Critical, High, Medium, Low, Informational, or Unknown**.

Step 4 Scans are performed on the devices based on the licenses associated against each device. In the **SCAN CRITERIA** area, you must follow the following order to match advisories against your devices:

- **Software Version:** Scans are performed on devices based on the software version with **Cisco DNA Essentials** license.
- **Custom:** Scans are performed on devices based on the software version and the custom configuration entered for an advisory (if any) against the device running configuration with **Cisco DNA Advantage** license.
- **Advanced:** Scans are performed on devices based on the software version, configuration, and operations data on devices with **Cisco CX Cloud Success Track** entitlements.

The license entitlements are not enforced in trial period and all devices are scanned at the **Advanced** level.

- Note**
- The security advisories dashboard shows security advisories published by Cisco that may affect devices on your network based on the software image currently installed. A further analysis of the configuration, platform details, or other criteria is required to determine if a vulnerability is actually present.
 - Security advisories scanning is only available for routers and switches that are running the minimum supported software version. For more information, see the [Cisco DNA Center Compatibility Matrix](#).
 - The security advisories displayed are subject to the [Cisco Security Vulnerability Policy](#).

The following table describes the information that is available.

Column	Description
Advisory ID	ID of the security advisories found in the network. Click the ID to go to the respective advisory web page.
Advisory title	Name of the security vulnerability advisory applicable to the network devices.
CVSS score	Score evaluated based on the Common Vulnerability Scoring System (CVSS) model.
Impact	Impact of the vulnerability on the network.
CVE	Common Vulnerabilities and Exposures (CVE) identifier for the vulnerability.

Column	Description
Devices	The number of devices impacted by the vulnerability. Click the number to view the devices that may be vulnerable based on this specific advisory, and upgrade the devices as needed.
Match Type	Indicates whether the vulnerability was detected based on the Image Version match or the Configuration match.
Known since (days)	The number of days since the vulnerability was discovered.
Last updated	The date when the advisory was last updated.

Step 5 The **FAILED DEVICES** area displays the information about the device scan scheduled for a later date and time.

Note The **FAILED DEVICES** area appears only when there is a failed device in a scan and system schedules a scan automatically.

Step 6 In the **Advisories** table click **All** tab to list all the advisories.

Step 7 In the **Advisories** table click **Affecting Devices** tab to view the advisories based on affecting devices.

The **Devices** table list the devices based on **Device Name**, **Device Family**, **Device Series**, **IP Address**, **Advisories**, **Advisories (Suppressed)**, **Platform**, **Image Version**, **Scan Status**, **Scan Criteria**, **Site**, and **Reachability**.

Step 8 Click the **Devices** tab to view the number of advisories applicable to each device.

- a) Click the number of advisories to view all that match the device.
- b) Click the topology icon in the top-right corner to view the device topology. You can click a device in the topology to view all advisories that match the device.

A lock icon next to the device indicates that there are one or more advisories applicable to the device.

The **Fixed Version** column shows the version in which the advisories are fixed. You can remove the advisory on your device by upgrading to the version mentioned in this column.

Step 9 Click **Re-scan Network** to run the scan the network again.

To re-scan the network to identify security advisories based on automated config scan, see [Rescan the Network to Identify Security Advisories, on page 695](#).

Schedule a Security Advisories Scan

Step 1 Click the menu icon (☰) and choose **Tools > Security Advisories**.

Step 2 Click **Scan Network**.

The **Scan Network** window appears.

Step 3 To scan the security advisories immediately, click the **Now** radio button and click **Start**.

Step 4 To schedule the scan for a later date and time, click the **Later** radio button and specify the date and time.

Step 5 Use the **Time Zone** drop-down list to schedule the scan according to a specific time zone.

- Step 6** Choose the recurrence option: **None** (the default), **Daily**, or **Weekly**.
- Step 7** In the **Run at Interval** field, enter the number of days or weeks for the recurrence of the scan.
- Step 8** (Optional) Check the **Set Schedule End** check box to schedule an end date and number of occurrences.
- To schedule a scan end date, click the **End Date** radio button and define the date and time.
 - To define the number of scan occurrences, click the **End After** radio button.
- Step 9** Click **Schedule**.
- Step 10** Click the menu icon (☰) and choose **Activities** > **Tasks** and confirm the schedule and recurrence of the scan.



Note In Cisco DNA Center releases earlier than 2.1.1.x, you have the ability to opt in or out of telemetry that Cisco collects. When you opt in, we collect your cisco.com ID, system telemetry, feature usage telemetry, network device inventory, and license entitlement. Telemetry is not application or feature specific; the disclosure of telemetry is for all of Cisco DNA Center. In Cisco DNA Center 2.1.1.x and later, telemetry collection is mandatory. The telemetry is designed to help the development of features that you use. See the [Cisco DNA Center Data Sheet](#) for a more expansive list of data that we collect.

When a security advisory scan runs, the following telemetry data is collected:

- Whether automatic update of knowledge packages has been set up.
- Whether recurring scanning and recurring reports have been set up.
- The number of reports that have been run.
- The number of devices with a security advisory match based on software version and configuration.
- The number of thumbs up/thumbs down votes, per scan.
- The manual configurations entered as a search, and the associated advisory.
- The number of advisory matches by software version and configuration, including product family.
- The number of devices based on other categories (zero advisories, unknown, and unsupported).
- The number of successful, failed, and terminated scans.
- The average scan time.

Enable the Try Cisco CX Cloud Success Track to Identify Security Advisories

Before you begin

- You must enter the correct URL and port in your firewall for Cisco DNA Center to reach the CX Cloud.
- You must enable the Cisco CX Cloud service. For more information, see **Update the Machine Reasoning Knowledge Base** in the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Tools > Security Advisories > Advisories**.
- Step 2** When you launch the **Security Advisories** window for the first time, click **Scan Network** to trigger an automated scan based on software version for all supported devices in the inventory.
- Step 3** In the banner at the top of the **Security Advisories** window, click the **Try Cisco CX Cloud Success Track** link to enable a 60-day trial of the CX license.
- Note** For security advisories, the CX license level is Success Track 1.
- Step 4** In the **Success Tracks** confirmation window, click **OK** to accept the end-user license agreement.
- At the top of **Security Advisories** window, a banner shows the validity of the CX license trial period.
-

CLI Commands Invoked for Security Advisories

Cisco DNA Center collects network device configuration and operational data by running CLI commands on network devices, and then sends the information to the CX Cloud to be processed for exposure to potential security advisories or bugs. Cisco DNA Center invokes the following CLI commands for security advisories:

- **show inventory**
- **show running-config**
- **show version**

Rescan the Network to Identify Security Advisories

The following procedure describes how to rescan the network to identify security advisories based on automated configuration scan.

Before you begin

You must enable the Cisco CX Cloud service. For more information, see **Update the Machine Reasoning Knowledge Base** in the [Cisco DNA Center Administrator Guide](#).

-
- Step 1** Click the menu icon (☰) and choose **Tools > Security Advisories > Advisories**.
- Step 2** Click **Re-Scan Network** to start the network scan again.
- Step 3** To rescan the security advisories immediately, click the **Now** radio button and click **Start**.
- Step 4** To schedule the rescan for a later date and time, click the **Later** radio button and specify the details. For information, see [Schedule a Security Advisories Scan, on page 693](#).
- In the **Device** table, the **Advisories** column is updated with the number of advisories.
- The Cisco DNA Center network rescan sends the running config of devices along with other details, such as platform details and the CX Cloud software version. The information is processed and sent back to Cisco DNA Center. The

Machine Reasoning Engine (MRE) running on Cisco DNA Center maps the advisories against the devices provided by the Cisco CX Cloud.

- If Cisco DNA Center cannot determine the correct license level for a given device, the security advisory scan falls back to scan by software version.

Hide and Unhide Devices from an Advisory

- Step 1** Click the menu icon (☰) and choose **Tools > Security Advisories**.
- Step 2** If you are launching the **Security Advisories** page for the first time, click **Scan Network**.
- Step 3** In the **Scan Network** window, choose **Now**, and then click **Start**.
- Step 4** To hide the devices from an advisory, do the following:
- From the **Focus** drop-down list, choose **Advisories**.
 - In the **Devices** column, click the devices count that corresponds to the advisory for which you want to hide the devices.
The **Active** tab shows the number of devices for which these advisories are issued.
 - Choose the devices that you want to hide and click **Suppress Device**.
The hidden devices can be viewed in the **Suppressed** tab.
 - Close the advisory window and view the change in the device count for this advisory.
- Step 5** To restore the devices to an advisory, do the following:
- From the **Focus** drop-down list, choose **Advisories**.
 - In the **Devices** column, click the devices count that corresponds to the advisory for which you want to unhide the devices.
 - Click the **Suppressed** tab to view the hidden devices.
 - Choose the devices that you want to unhide and click **Mark as Active**.
The restored devices can be viewed in the **Active** tab.
 - Close the advisory window and view the change in the device count for this advisory.
-

Hide and Unhide Advisories from a Device

- Step 1** Click the menu icon (☰) and choose **Tools > Security Advisories**.
- Step 2** If you are launching the **Security Advisories** page for the first time, click **Scan Network**.
- Step 3** In the **Scan Network** window, choose **Now**, and then click **Start**.
- Step 4** To hide the advisories for a device, do the following:
- From the **Focus** drop-down list, choose **Devices**.

- b) In the **Advisories** column, click the advisories count that corresponds to device for which you want to hide the advisories.

The **Active** tab shows the number of advisories issued for this device.

- c) Choose the advisories that you want to hide and click **Suppress Advisory**.

The hidden advisories can be viewed in the **Suppressed** tab.

- d) Close the device window and view the change in the advisory count for this device.

Step 5

To restore the advisories for a device, do the following:

- a) From the **Focus** drop-down list, choose **Devices**.
- b) In the **Advisories** column, click the advisories count that corresponds to the device for which you want to unhide the advisories.
- c) Click the **Suppressed** tab to view the hidden advisories.
- d) Choose the advisories that you want to unhide and click **Mark as Active**.

The restored advisories can be viewed in the **Active** tab.

- e) Close the device window and view the change in the advisories count for this device.

Add Notification for a New Security Advisory KB

A security advisory Knowledge Bundle (KB) uses a Machine Reasoning Engine (MRE) to scan the network. You can configure Cisco DNA Center to notify you when a new security advisory KB is available. After you enable notifications, Cisco DNA Center displays a visual notification and actionable alert whenever a new security advisory KB is available.

The following procedure explains how to add notifications for new security advisory KBs:

Before you begin

- You must install the Cisco DNA Center core package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- You must install the Machine Reasoning (MRE) package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
- The following containers must be present in your system:
 - cnsr-reasoner
 - cloud connectivity/download

Step 1 Click the notification icon in the top-right corner of the Cisco DNA Center GUI. From the drop-down menu, select the gear icon to view the notification preferences.

Step 2 In the **My Profile and Settings** window, enable the security advisory notification by choosing the **Security Advisories** option.

Step 3 Click **Save**.

- Step 4** In the **Machine Reasoning Engine** window, click the **Download Latest** link to download the latest knowledge bundle.
- Step 5** Review and update the Knowledge Base settings.
- Step 6** In the **Security Advisory Settings** section, choose the recurrence option: **None** (default), **Daily**, or **Weekly**.
- Step 7** Choose **Notification Center** > **Go to Security Advisories** to view the Security Advisories tool window directly.
- Step 8** Rescan the network with the newly downloaded security advisories. For more information, see [Schedule a Security Advisories Scan](#), on page 693.
-

View Security Advisories in the Inventory

The Cisco DNA Center security focus view lists the security advisories for your devices, based on the data retrieved from the previous security scan. The device data that you retrieve from the **Security Advisories** tool is displayed in the **Inventory** window.

Use the following procedure to view the security advisories:

Before you begin

- You must install the Cisco DNA Center core package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
 - You must install the Machine Reasoning package. See Download and Install Packages and Updates in the [Cisco DNA Center Administrator Guide](#).
-

- Step 1** Click the menu icon (☰) and choose **Tools** > **Security Advisories**.
- Step 2** Click **Scan Network**.
- Step 3** To scan the security advisories immediately, click the **Now** radio button and click **Start**.
- Step 4** Click the menu icon (☰) and choose **Provision** > **Network Devices** > **Inventory**.
- Step 5** From the **FOCUS: Inventory** drop-down menu, choose **Security**. The **Advisories** column is displayed in the **Inventory** table.
- Step 6** In the **Device Details** window, select a device and view the advisories data.
- Step 7** Click **Manage All** to navigate to the **Security Advisories** tool.
-

Add a Match Pattern

- Step 1** Click the menu icon (☰) and choose **Tools** > **Security Advisories**.
- Step 2** If you are launching the **Security Advisories** page for the first time, click **Scan Network**.
- Step 3** In the **Scan Network** window, choose **Now**, and then click **Start**.
- Step 4** Choose an advisory and in the **Match Type** column, click **Add match pattern**.

- Step 5** In the **Add Configuration Match Pattern** window, enter the condition to match with devices in the **CONDITIONS** text box.
- Step 6** Click **Save**.
The match pattern is added to the advisory.
- Step 7** Click **Scan Network** to check the number of devices that match with the match pattern.
-

Define AND/OR for the Match Pattern

- Step 1** Click the menu icon (☰) and choose **Tools > Security Advisories**.
- Step 2** If you are launching the **Security Advisories** page for the first time, click **Scan Network**.
- Step 3** In the **Scan Network** window, choose **Now**, and then click **Start**.
- Step 4** Choose an advisory and in the **Match Type** column, click **Add match pattern**.
- Step 5** In the **Add Configuration Match Pattern** window, do the following:
- In the **CONDITIONS** text box, enter a condition and then click the **Add** icon.
 - From the drop-down list, choose **AND** or **OR** and then enter the next condition.
 - If you want to delete a condition, click the **Remove** icon.
 - Click **Save**.
The match pattern is added to the advisory.
- Step 6** Click **Scan Network** to check the number of devices that match the match pattern.
-

Edit the Match Pattern

- Step 1** Click the menu icon (☰) and choose **Tools > Security Advisories**.
- Step 2** If you are launching the **Security Advisories** page for the first time, click **Scan Network**.
- Step 3** In the **Scan Network** window, choose **Now**, and then click **Start**.
- Step 4** Choose an advisory that already has a match pattern and in the **Match Type** column, click **Edit match pattern**.
- Step 5** In the **Edit Configuration Match Pattern** window, enter the condition to match with devices in the **CONDITIONS** text box.
- Step 6** Click **Save**.
The match pattern is changed.
- Step 7** Click **Scan Network** to check the number of devices that match the match pattern.
-

Delete the Match Pattern

- Step 1** Click the menu icon (☰) and choose **Tools > Security Advisories**.
- Step 2** If you are launching the **Security Advisories** page for the first time, click **Scan Network**.
- Step 3** In the **Scan Network** window, choose **Now**, and then click **Start**.
- Step 4** Choose an advisory that already has a match pattern and in the **Match Type** column, click **Edit match pattern**.
- Step 5** In the **Edit Configuration Match Pattern** window, click **Delete**.
- The match pattern is deleted.
-



PART **VIII**

Assure Your Network

- [Cisco DNA Assurance, on page 703](#)



CHAPTER 30

Cisco DNA Assurance

- [Overview of Cisco DNA Assurance, on page 703](#)

Overview of Cisco DNA Assurance

Cisco DNA Assurance is an application that is available from Cisco DNA Center.

For details about the Assurance application, including how to monitor and troubleshoot network health, client health, and application health, and enable NetFlow collection, see the [Cisco DNA Assurance User Guide](#).



PART **IX**

Manage Cisco DNA Center

- [Build and Deploy Workflows, on page 707](#)
- [Troubleshoot Cisco DNA Center Using Data Platform, on page 739](#)



CHAPTER 31

Build and Deploy Workflows

- [Cisco DNA Center Workflow Navigation, on page 707](#)
- [Discover Devices, on page 707](#)
- [AP Refresh Workflow, on page 709](#)
- [Configure User-Defined Network Workflow, on page 711](#)
- [Enable Application Hosting on Switches, on page 714](#)
- [Enable IoT Services Workflow, on page 715](#)
- [AP Configuration in Cisco DNA Center, on page 716](#)
- [Learn Device Configurations from Devices with Pre-Existing Infrastructure, on page 724](#)
- [Replace Device Workflow, on page 729](#)
- [Create a Remote Support Authorization, on page 731](#)
- [Create an Event Notification, on page 732](#)
- [Configure Remote LAN, on page 735](#)
- [Workflow to Create an IP- and URL-Based Access Control Policy, on page 737](#)

Cisco DNA Center Workflow Navigation

Cisco DNA Center workflows are similar to wizards. The workflows are embedded in the GUI to guide you through multistep tasks that would otherwise be too complex or advanced to complete. You can access many of them from various menu options or directly from the **Workflows** menu option.

Use these guidelines to help you navigate through the workflows:

- Follow the steps in the workflow and click **Next** to go to the next page.
- When you hover your cursor near the top of each page in the workflow, a **Progress bar** displays, showing you the steps to complete the process and which step you are currently on.
- Some workflows open a dialog box that you can click through to see a visual overview of the task. At any point in the task overview, you can click **Let's Do it** to jump directly to the beginning of the workflow.

To skip the task overview in the future, check the **Don't show this to me again** check box.

Discover Devices

This workflow guides you from device discovery to network health.

Before you begin

- Your devices must have the required device configurations, as described in [Discovery Prerequisites, on page 38](#).
- Enable CDP on your network devices, if you want to use CDP discovery protocol.
- Enable LLDP on your network devices, if you want to use LLDP discovery protocol.
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Discover Devices**.
- Step 2** If a task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 3** In the **Let's Get Ready** window, click **Next**.
- Step 4** In the **Discover Devices** window, complete the following fields:
- a) Enter a name for the discovery job.
 - b) Under **Discovery Type**, choose the protocol used to discover devices and complete the corresponding fields, as follows:
 - **CDP**: Enter the **IP Address**, **CDP Level**, and **Subnet Filter**.
 - **IP Address Range**: Enter the **Starting IP Address** and **Ending IP Address**.
 - **LLDP**: Enter the **IP Address**, **LLDP Level**, and **Subnet Filter**.
 - c) Choose the **Preferred Management IP Address**.
- Step 5** In the **Provide Credentials** window, enter at least one CLI credential and one SNMP credential that Cisco DNA Center will configure for the devices it discovers. You can have a maximum of five global credentials and one task-specific credential for each type. For more details, see [Discovery Credentials, on page 39](#).
- Step 6** In the **Advanced Settings** window, do the following:
- a) **Protocol Order**: Choose **SSH** or **Telnet**. If you choose both, you can specify the order in which they are used by dragging the protocols up or down.
 - b) Configure the **SNMP Polling Properties**. Use the global SNMP polling properties defined in the **Network Settings > Device Credentials** window or modify for this discovery instance.
- Step 7** In the **Assign Devices to Site** window, do any one of the following:
- **Assign devices to an existing site**: Use the **Search Hierarchy** search field or the filter icon to find a site, building, or area. For more details, see [Search the Network Hierarchy, on page 134](#)
 - **Assign devices to a new site**: Click the **Already have an area** radio button or **Create a new area** radio button and complete the required fields.
 - **Skip site assignment for now**: Use this option if you want the devices to be assigned to sites later from inventory.
- Step 8** In the **Schedule Task** window, do the following:
- a) Click the toggle button to enable or disable **Discover new devices only** option.
 - b) Click **Now** to start device discovery immediately or click **Later** to schedule device discovery at a specific time.
- If you choose **Daily** or **Weekly** recurrence option, the **Discover new devices only** option will be disabled.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Start Discovery and Telemetry**.

You can view the status of the task in the **Activity** page.

AP Refresh Workflow

The AP Refresh feature allows you to replace both provisioned and unprovisioned older AP models with newer AP models, using the Access Point Refresh workflow. You can use the following procedure to replace old APs with new ones in Cisco DNA Center.

For device compatibility information, see the [Cisco DNA Center Compatibility Matrix](#).

Before you begin

- Ensure that the old AP is in Unreachable state and assigned to a site.
 - The old AP site must be provisioned as a managed AP location for the wireless controller to which the new AP is associated.
 - The new AP must not be assigned to any site.
 - You must connect the new AP to a Cisco Wireless Controller. The new AP must either be available in the Cisco DNA Center inventory or be able to contact Cisco DNA Center through Plug and Play (PnP). It must be in Reachable state.
-

Step 1 Click the menu icon (☰) and choose **Workflows > Access Point Refresh**.

Note If an **Overview** window opens, click **Let's Do it** to start the workflow.

Step 2 In the **Get Started** window, enter a unique name for the task and click **Next**.

Step 3 In the **Select Access Points** window, do the following:

- a. In the left pane, check the check box next to the floor where you want to refresh the AP.
- b. In the right pane, check the check box next to the device name that you want to replace.

Step 4 In the **Assign New APs to Old APs** window, select a method through which you want to provide new AP details:

- To add the new AP details using the GUI, click the edit icon (✎) for the AP, and in the **Edit details** window, do the following:
 - a. (Optional) Update the new AP name.
 - b. (Optional) From the **Choose Platform ID** drop-down list, choose the platform of the new AP.
 - c. From the **Choose Serial Number** drop-down list, choose the serial number of the new AP.

If the new AP is already associated with a wireless controller and is available in the inventory, Cisco DNA Center displays the serial number of that AP as **Managed** in the **Choose Serial Number** drop-down list.

If the new AP has contacted Cisco DNA Center through PnP, Cisco DNA Center displays the serial number of that AP as **Unclaimed** in the **Choose Serial Number** drop-down list.

If the serial number of the new AP is not available in the Inventory, the **Serial Number** drop-down list doesn't contain the serial number. To add a new serial number that is not present in the inventory, from the **Choose Serial Number** drop-down list, enter the serial number and click +.

d. Click **Save**.

- To add the new AP details using comma-separated value (CSV) file, do the following:
 - a. Click **Download CSV**. The downloaded CSV template file contains the old AP details. Update the device name and add the serial number of the new AP.
 - b. To import the CSV file, click **Upload CSV**.
 - c. In the **Upload CSV** window, you can either drag and drop the CSV file into the drag-and-drop area or click **Choose a file**, browse to the location of the CSV file, and click **Open**.

Cisco DNA Center performs a validation check. If the uploaded CSV file doesn't meet the requirement, an error message appears. Click **View Details** to get more details about the error message.

d. Click **Upload**.

Step 5 In the **Configuration to be copied from Old APs to New** window, view the configuration that will be copied from the old AP to the new AP.

Step 6 If Cisco DNA Center detects any errors or unresolved dependencies, the **Resolve Dependencies** window is displayed. You must resolve any errors and dependencies before proceeding, including the following:

- **Device EULA Acceptance:** Accept the device End-User License Agreement (EULA) by providing your Cisco.com credentials.
- **Update the Cisco Wireless Controller software image version:** You must resolve this dependency even though it doesn't stop you from proceeding with the AP refresh.
- **AP Connected SwitchPort:** You must resolve this dependency even though it doesn't stop you from proceeding with the AP refresh.

Step 7 In the **Schedule Access Point Refresh Task** window, click **Now** or **Run Later** to schedule the AP refresh task for a later date and time.

Step 8 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 9 In the **Track Replacement Status** window, monitor the AP replacement status:

- If the AP replacement succeeds, the **Replacement Status** shows **REPLACED**.
- If the AP replacement fails, the **Replacement Status** shows **Error**.

Note If the new AP is not yet discovered in the inventory and the corresponding AP refresh entry is waiting for the new device to be connected, or if the PnP claim process is in progress, resynchronize the Cisco Wireless Controller.

Step 10 (Optional) In the **Track Replacement Status** window, do any of the following:

- To view the latest AP replacement status, click **Refresh Data**.

- To get more information about the AP replacement status, click **View Details**.
- To delete a replacement entry, under the **Actions** column, click the three blue dots and click **Delete**. In the **Warning** dialog box, click **Yes**.
- To download the provisioning summary to a CSV file that you can save locally, click **Export**.
- To download the provisioning status report, click **Download Report**.

Step 11 Click **Next** to view the refresh summary.

After a successful replacement, an AP refresh event is generated in Cisco DNA Assurance for the old and new APs.

Step 12 (Optional) View the AP refresh event under **Event Viewer** in the **AP View 360** window.

Cisco DNA Center automatically updates the new APs on the respective floor maps in the **Network Hierarchy** window.

Configure User-Defined Network Workflow

The following sections provide information about configuring the Cisco User-Defined Network service using workflows in Cisco DNA Center.

Overview of User-Defined Network Service

Home, consumer, and IoT devices on the network, such as printers, speakers, Apple TV, Google Chromecast, ring doorbells, smart bulbs, and so on, depend on the Simple Service Discovery Protocols (SSDP) such as Apple Bonjour, multicast DNS (mDNS), and Universal Plug and Play (UPnP) to provide the easy discovery and usage of devices.

The Cisco User-Defined Network service provides secure and remote onboarding of client devices in shared environments such as dormitory rooms, residence halls, class rooms, and auditoriums. With the User-Defined Network service, users can securely use SSDPs such as Apple Bonjour, mDNS protocols such as AirPlay, AirPrint, Screen Mirroring, Print, or UPnP protocol to interact and share with only their registered device in the shared environment.

The User-Defined Network service provides the following solution:

- Easy and secure onboarding of client devices.
- Automatic segmentation of client devices that belong to a particular user.
- Ability to invite other users to share their devices.

Prerequisites for Configuring the User-Defined Network Service

Before configuring the Cisco User-Defined Network service, the following prerequisites must be completed:

- Confirm that APs have joined the Cisco Wireless Controller.
- Discover Cisco Wireless Controllers and APs in your network using the **Discovery** functionality so that the discovered devices are listed in the **Inventory** window.

- Map the AAA server client endpoint with Cisco Identity Services Engine.
- Add the authentication tokens to Cisco DNA Center.
- Create nonfabric enterprise SSIDs or guest wireless SSIDs with any security, and map them to the network profile.
- Provision SSIDs.

Configure Cisco User-Defined Network

This procedure shows how to configure the Cisco User-Defined Network (UDN) using workflows.

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure Cisco UDN**.
Alternatively, you can configure the Cisco UDN from **Provision > Services > Cisco User Defined Network**.
- Step 2** If a task overview window opens, click **Let's Do It** to go directly to the workflow.
- a) Click **Click here**.
The **Cloud Authentication** window opens.
 - b) Hover over **Where did I get my token encryption key?** and click **Go to the Portal**.
The **Cisco DNA - Cloud** application opens in a new tab.
 - c) Log in to Cisco DNA - Cloud using your Cisco.com account ID and password.
The **Cisco DNA - Cloud** home window lists the subscribed offers for your region as a card.
- Step 3** Generate an authentication token using the Cisco DNA Cloud portal to allow Cisco DNA Center to connect with Cisco DNA Cloud:
- a) In the **Cisco DNA - Cloud** GUI, click the menu icon (☰) and choose **Applications > Product** to register Cisco DNA Center to your cloud subscription.
By default, the **ALL** tab opens and is highlighted with a blue tick mark. You can register either from the **ALL** tab or from the **Cisco DNA Center** tab.
Note Cisco DNA Center registration fails intermittently on the Cisco DNA - Cloud portal. This is an intermittent issue that occurs during every alternate deregistration due to communication failure from Cisco DNA - Cloud to Cisco DNA Center in all regions.
 - b) To register from the **ALL** tab:
 - Click **Register**.
The **Register Product** slide-in pane appears.
 - In the **Product Name** field, enter a name.
 - From the **Product Type** drop-down list, choose **Cisco DNA Center**.
 - Click **Register**.
 - The **OTP Generated** dialog box appears after successful registration of Cisco DNA Center. To copy the OTP, click **Copy**, and click **close**.

- c) Alternatively, to register from the **Cisco DNA Center** tab:
- Click **Register** to securely connect your products to the relevant cloud applications and services offered by Cisco and its partners.
- The **Register Product** slide-in pane appears.
- In the **Cisco DNA Center Name** field, enter the name of the on-premises Cisco DNA Center.
 - In the **OTP Generated** dialog box, click **Copy** to copy the OTP and click **close**.

Step 4 Navigate back to the **Cloud Authentication** window to establish the connection:

- a) In the Cisco DNA Center GUI, click the menu icon (☰) and choose **System > Settings > External Services > Cloud Authentication**.
- b) Click **Add OTP Key**.
- c) In the **OTP Code** field, paste the OTP that you generated and copied in the Cisco DNA - Cloud application, and click **Done**.
- d) In the **Success** dialog box, click **OK**.

Step 5 Verify whether the connection has been established between **Cisco DNA Center** and **Cisco DNA - Cloud** on the **Cisco DNA - Cloud > Applications > Products** window.

The **Registration Status** column shows the status as **Registered** after a successful registration.

Step 6 Enable sites and provision Cisco UDN services on your network:

- a) Navigate back to the **Welcome to Cisco User Defined Network** window in Cisco DNA Center.
- b) Click **Next**.
- c) In the **Select Sites** window, choose the sites where you want to enable the Cisco UDN service.
- d) In the **SSID(s)** window, do the following:
 - From the **SSID(s)** drop-down list, choose the SSIDs where you want to enable the Cisco UDN service.
 - To limit the unicast traffic for the selected SSID, turn on **Unicast Traffic Containment**.
 - Click **Apply Individually** to apply unicast traffic containment for a specific site.
 - Click **Apply to all** to apply the unicast traffic containment for all sites.
 - Click **Next**.

Step 7 In the **Scheduling** window, click **Now** or **Later** to indicate when you want to provision the Cisco UDN service. Then, click **Next**.

Step 8 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

- a) Expand the **Connection Status** area to view the connection status between Cisco DNA Center and Cisco UDN Cloud.
A "Paired with Cisco DNA - Cloud" message appears after establishing a connection between Cisco DNA Center and Cisco UDN Cloud.
- b) Click **Configure**.
In the next window, a check mark is shown next to each step as it completes.

Enable Application Hosting on Switches

The following procedure shows how to enable docker applications such as ThousandEyes Enterprise Agent and iPerf in selected switches at a specific site.

Before you begin

- Complete the prerequisites. For more information, see [Prerequisites for Application Hosting, on page 530](#).
- Add the application to Cisco DNA Center. For more information, see [Add an Application, on page 531](#).
- Check the readiness of the switch to host the application. For more information, see [View Device Readiness to Host an Application, on page 531](#).

Step 1 Click the menu icon (☰) and choose **Provision > App Hosting for Switches**.

Step 2 Choose the application and click **Install** at the bottom of the window.

Alternatively, you can also launch the workflow by choosing **Workflows > Enable Apps on Switches > Let's Do it**.

Note At the top of the workflow window, place your cursor on the blue progress bar and switch back to the previous step listed.

Step 3 In the **Select Site** window, navigate to the building where you want to enable the application.

Step 4 In the **Select App** window, click on the application you want to select.

Note You can access the + **New App** link to add an application that is not present in Cisco DNA Center.

Step 5 In the **Select Switches** window, check the check box next to the device name for which you want to enable the application.

Note You can import or export devices in bulk by providing the details in the specified template in the **Select Switches** dialog box.

Step 6 Complete the following settings in the **Configuration App** window:

- **App Networking**
 - **Device Network:** From the **Select Network** drop-down list, choose a VLAN to configure the application.
 - **App IP address:** From the **Address Type** drop-down list, choose **Static** or **Dynamic**. If you choose **Static**, click the thumbnail icon and enter the **IP Address**, **Gateway**, **Prefix/Mask**, and **DNS** for the application.
- **Resource Allocation:** Check the **Allocate resources as asked by the app** or the **Allocate all resources available on the device** check box.
- **Custom Settings:** (Applicable only for Cisco package applications) Enter the configuration details for the attributes that are specified by the application.
- **App Data:** Browse and upload the application-specific files. To identify the required application-specific files, see the relevant application document.
- **Docker Runtime Options:** Enter the docker runtime options required by the application.

- Step 7** In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)
The **Provisioning Task** window displays the task name that tracks the deployment of the application on the switches.
- Step 8** Review the automatically generated task name and click **Provision**.
- Step 9** In the **Track Provisioning Status** window, you can track the progress of the deployment.
- Step 10** Click **View Details** to view the provisioning status of the individual devices and failures, if any and click **Next**.
The application is enabled successfully.
The summary of the task result and the success/failure counts are displayed.
- Step 11** Click **Manage App**, where you can manage the lifecycle operations of the application to perform Day N tasks.
-

Enable IoT Services Workflow

The following sections provide information about enabling IoT technologies such as Bluetooth, Zigbee, and ESL on Cisco Catalyst 9100 Series Access Points using **Workflows** in Cisco DNA Center.

Enable IoT Services on Cisco Catalyst 9100 Series Access Points

This procedure shows how to enable IoT technologies such as Bluetooth, Zigbee, and ESL on selected Catalyst 9100 Series Access Points.

- Step 1** Click the menu icon (☰) and choose **Workflows > Enable IOT Services**.
- Step 2** If a task overview window opens, click **Let's Do It** to go directly to the workflow.
- Step 3** In the **Select Site** window, navigate to the floor where you want to enable the IoT service, and click **Next**.
- Step 4** In the **Select the Application** window, select the SES-imagotag ESL Connector application to enable IoT in your network, and click **Next**.
- Note** To add an application that is not present in the Cisco DNA Center, see [Add an Application](#).
- The **Select Access Points** window shows all the APs available on the particular floor.
- Step 5** In the **Select Access Points** window, check the check box adjacent to the **Device Name** where you want to install the IoT connector application, and click **Next**.
- Step 6** In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)
- Step 7** The **Provisioning Task** window, which displays the task name created to track deployment of any application on APs, is displayed. Review the auto-generated task name and click **Provision**.
- Step 8** In the **Track Provisioning Status** window, you can track the progress of the deployment. Click **View Details** to view the provisioning status and click **Next**.
- Step 9** The **Done! Task Completed** window appears. Click **Manage IoT Application** to perform Day N tasks.
-

Manage IoT Applications

This procedure shows how to manage IoT applications.

Before you begin

You must have enabled IoT services on Cisco Catalyst 9000 Series Access Points.

-
- Step 1** After enabling IoT services, click **Manage IoT Application** in the **Done! Task Completed** window.
- Step 2** Check the check box next to the **Hostname** and perform the following tasks:
- To start the application, from the **Actions** drop-down list, choose **Start App**.
 - To stop the application, from the **Actions** drop-down list, choose **Stop App**.
 - To edit the application configuration, from the **Actions** drop-down list, choose **Edit App Config**.
 - To upgrade the application, from the **Actions** drop-down list, choose **Upgrade App**.
 - To uninstall the application from the selected AP, from the **Actions** drop-down list, choose **Uninstall App**.
- Step 3** Click the AP name to view details, such as the AP name, status, IP address, and health.
- Step 4** Click **Tech Support logs** to collect Application Hosting logs.
-

AP Configuration in Cisco DNA Center

The **Configure Access Points** workflow allows you to configure and deploy AP-level parameters, such as the AP location, admin status, mode, and so on. You can also configure radio-level parameters, such as the radio power level, channel settings, and so on.

Configure AP Workflow

This procedure shows how to configure AP and radio parameters in Cisco DNA Center.

The following settings configured using the **Configure Access Points** workflow aren't overwritten when the wireless controller or APs are reprovisioned:

- Admin status for radios (only applicable for Cisco AireOS Wireless Controllers)
- AP primary controller
- AP secondary controller

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure Access Points**.
If an Overview window is displayed, click **Let's Do It** to go directly to the workflow.
- Step 2** In the **Get Started** window, enter a unique name for the workflow in the **Task Name** field and click **Next**.
- Step 3** In the **How do you want to configure APs?** window, do the following:

- a) Click the **Configure AP And Radio Parameters** radio button.
- b) Check the check box next to the tasks that you want to perform:

- **Modify AP Name**
- **Configure AP Parameters**
- **Configure 5 GHz Radio Parameters**
- **Configure 2.4 GHz Radio Parameters**
- **Configure 6 GHz Radio Parameters**
- **Configure Dual-Band (XOR) Radio Parameters**
- **Configure Tri-Radio Parameters**

Note Based on the check boxes that you check, Cisco DNA Center displays the corresponding subsequent configuration steps.

- c) Click **Next**.

Step 4

In the **Select Access Points** window, do the following:

- a) Navigate to the site where you want to apply AP-related configurations.
The right pane lists all the APs available in the selected site.
- b) Check the check boxes next to the AP names that you want to configure.
- c) Click **Next**.

We recommend that you select a maximum of 2000 APs in this window.

Note Effective with Release 2.3.5.3, you can select up to 2000 sites in this window.

Step 5

(Optional) In the **Modify AP Name** window, modify one or more AP names using one of the following methods:

- **Create a New Naming Convention:** Click this radio button, enter a name based on your naming convention, and click **Apply Pattern**. The **Access Points** table shows the new AP names based on the naming pattern that you entered.
- **Upload a CSV file:** Click this radio button, download the sample CSV template file, and add your AP names to it. Then, upload the CSV file either by dragging and dropping it into the drop area or by clicking **Choose a file** and browsing to select it.

Step 6

(Optional) In the **Configure AP Parameters** window, configure the AP parameters.

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
- **AP Mode:** Check this check box and choose the AP mode from the **Select AP Mode** drop-down list. Valid modes are **Local/Flexconnect**, **Monitor**, **Sniffer**, and **Bridge/Flex+Bridge**.

Note When you change the AP mode from **Monitor** or **Sniffer** to **Local/Flexconnect**, Cisco DNA Center uses the following settings:

If **FlexConnect Local Switching** is enabled on any associated SSID, Cisco DNA Center sets **FlexConnect** mode on the AP. Otherwise, it sets **Local** mode on the AP.

For unassigned APs or APs that are assigned but not provisioned, Cisco DNA Center sets **FlexConnect** mode on the AP as follows:

- For Cisco AireOS Wireless Controller: If **FlexConnect Local Switching** is enabled on any associated SSID in the AP group where the AP is present.
- For Cisco Catalyst 9800 Series Wireless Controller: If **Local site** is disabled on the current associated site tag of the AP.

- **AP Location:** Check this check box to enter the AP location details in the **Enter Location** field.

To use the currently assigned site as the AP location, check the **Use currently assigned site location** check box. If you check this check box, the **Enter Location** field is disabled. You can view the AP location that is being configured for each AP using the **Preview the CLI** link in the **Summary** window of this workflow before pushing this change to the device.

Note If you check the **Use currently assigned site location check box**, for APs that are not assigned to any site, Cisco DNA Center doesn't configure the AP location.

- **AP LED Status:** To disable the APs LED status, check this check box and click **Disable**.
- **LED Brightness Level:** Check this check box and choose the brightness level from the **LED Brightness Level**.
- **AP Failover Priority:** Check this check box and, from the **AP Failover Priority** drop-down list, choose one of the following failover priorities:
 - **Low** (Default): Level 1 priority, which is the lowest priority level.
 - **Medium:** Level 2 priority.
 - **High:** Level 3 priority.
 - **Critical:** Level 4 priority, which is the highest priority level.
- **High Availability:** Check this check box and configure the primary, secondary, and tertiary controller name and the IP address for the AP.

If you choose **Inherit from site** / **Clear** for the primary and secondary controllers:

- For the APs that are in Provisioned state, the controllers that are configured as primary and secondary for the floor where the AP is assigned are configured as the primary and secondary controllers on the AP.
- For the APs that are not in Provisioned state, the current primary and secondary controller configuration is cleared from the AP.

For the tertiary controller, only the **Clear** option is available.

- Note**
- If AP fallback is disabled on the controller, the AP doesn't join the newly configured primary, secondary, and tertiary controller.
 - If the AP is a ROW AP, ensure that you have added support for the country of operation to the country list on the controller. You must configure at least one site from the country of operation as the managed AP location for the controller.

Note Effective with Cisco DNA Center Release 2.3.5.3, the **AP Height** parameter is no longer available in the **Configure Access Points** workflow. You can configure the AP height in the **Design > Network Hierarchy** window. For more information, see [Edit an AP, on page 152](#).

Step 7

(Optional) In the **Configure 5 GHz Radio Parameters** window, configure the 5-GHz radio parameters.

- a) To view the list of applicable APs for the 5-GHz radio parameter configuration, click **View Devices**.

Cisco DNA Center displays the **View Devices** option only when APs that support 5-GHz radio parameters are available.

- b) Configure the following 802.11 a/n/ac/ax parameters:

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
- **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.
- **Channel Assignment:** To choose custom channel numbers, check this check box and click the **Custom** button. Choose a custom channel number from the **Select Custom Channel** drop-down list.
- **Channel Width:** To choose channel width, check this check box and choose the channel bandwidth.
- **CleanAir / Spectrum Intelligence:** To disable CleanAir spectrum intelligence, check this check box and click **Disable**.
- **Antenna Gain:** To choose an antenna gain, check this check box and choose an antenna from the **Select Antenna** drop-down list. If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 through 40.

Note The selected antenna name isn't reflected in wireless maps.

- **Antenna Cable:** To choose an antenna cable, check this check box and choose the antenna cable from the **Select Antenna Cable** drop-down list. If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 through 40.

Note Effective with Cisco DNA Center Release 2.3.5.3, the **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure the azimuth and elevation in the **Design > Network Hierarchy** window. For more information, see [Edit an AP, on page 152](#).

Step 8

(Optional) In the **Configure 2.4 GHz Radio Parameters** window, configure the 2.4-GHz radio parameters.

- a) To view the list of applicable APs for the 2.4-GHz radio parameter configuration, click **View Devices**.

Cisco DNA Center displays the **View Devices** option only when APs that support 2.4-GHz radio parameters are available.

b) Configure the following 802.11 b/g/n parameters:

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
- **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.
- **Channel Assignment:** To choose custom channel numbers, check this check box and click the **Custom** button. Choose a custom channel number from the **Select Custom Channel** drop-down list.
- **CleanAir / Spectrum Intelligence:** To disable CleanAir spectrum intelligence, check this check box and click **Disable**.
- **Antenna Gain:** To choose an antenna gain, check this check box and choose an antenna from the **Select Antenna** drop-down list. If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 through 40.

Note The selected antenna name isn't reflected in wireless maps.

- **Antenna Cable:** To choose an antenna cable, check this check box and choose the antenna cable from the **Select Antenna Cable** drop-down list. If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 through 40.

Note Effective with Cisco DNA Center Release 2.3.5.3, the **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure the azimuth and elevation in the **Design > Network Hierarchy** window. For more information, see [Edit an AP, on page 152](#).

Step 9

(Optional) In the **Configure 6 GHz Radio Parameters** window, configure the 6-GHz radio parameters.

a) To view the list of applicable APs for the 6-GHz radio parameter configuration, click **View Devices**.

Cisco DNA Center displays the **View Devices** option only when APs that support 6-GHz radio parameters are available.

b) Configure the following parameters:

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
- **Radio Role Assignment:** To choose a radio role, check this check box and click the **Auto**, **Client-Serving**, or **Monitor** button.
- **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.
- **Channel Assignment:** To choose a custom channel number, check this check box and click the **Custom** button. Choose a custom channel number from the **Select Custom Channel** drop-down list.
- **Channel Width:** To choose channel width, check this check box and choose the channel bandwidth.

Note Effective with Cisco DNA Center Release 2.3.5.3, the **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure the azimuth and elevation in the **Design > Network Hierarchy** window. For more information, see [Edit an AP, on page 152](#).

Step 10 (Optional) In the **Configure Dual-Band (XOR) Radio Parameters** window, configure the dual-band (XOR) radio parameters.

- a) To view the list of applicable APs for the dual-band (XOR) radio parameter configuration, click **View Devices**. Cisco DNA Center displays the **View Devices** option only when APs that support dual-band (XOR) parameters are available.

You can configure dual-band (XOR) radio parameters on the following APs:

- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9120 Series Access Points
- Cisco Catalyst 9166 Series Access Points

Note Cisco Catalyst 9166 Series Access Point supports dual-band (XOR) between 5-GHz and 6-GHz radio modes. The other APs support dual-band (XOR) between 2.4-GHz and 5-GHz radio modes.

- b) Configure the following parameters:

- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
 - **Radio Role Assignment:** To choose a radio role, check this check box and click the **Auto**, **Client-Serving**, or **Monitor** button. Click the required option for radio band.
 - **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.
 - **Channel Assignment:** To choose a custom channel number, check this check box and click the **Custom** button. Choose a custom channel number from the **Select Custom Channel** drop-down list.
 - **Channel Width:** To choose channel width, check this check box and choose the channel bandwidth.
 - **CleanAir:** To disable CleanAir spectrum intelligence, check this check box and click **Disable**.
 - **Antenna Gain:** To choose an antenna gain, check this check box and choose an antenna from the **Select Antenna** drop-down list. If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 through 40.
- Note** The selected antenna name isn't reflected in wireless maps.
- **Antenna Cable:** To choose an antenna cable, check this check box and choose the antenna cable from the **Select Antenna Cable** drop-down list. If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 through 40.

Note Effective with Cisco DNA Center Release 2.3.5.3, the **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure the azimuth and elevation in the **Design > Network Hierarchy** window. For more information, see [Edit an AP, on page 152](#).

Step 11 (Optional) In the **Configure Tri-Radio Parameters** window, configure the tri-radio parameters.

- a) To view the list of applicable APs for the tri-radio parameter configuration, click **View Devices**.

- Note**
- Cisco DNA Center displays the **View Devices** option only when APs that support tri-radio parameters are available.
 - Cisco DNA Center doesn't support tri-radio parameter configuration for APs that are in **Monitor** or **Sniffer** modes.

You can configure tri-radio parameters for the following APs:

- Cisco Catalyst 9124AXE Series Access Points
- Cisco Catalyst 9130AXI Series Access Points
- Cisco Catalyst 9130AXE Series Access Points

- b) Configure the following parameters:

- **Dual Radio Mode:** To choose the dual radio mode, check this check box and click **Auto**, **Enable**, or **Disable**.

Note When you enable dual radio mode, global tri-radio mode is enabled on the corresponding wireless controllers.

- **Radio Role Assignment:** To choose a radio role, check this check box and click **Auto**, **Client-Serving**, or **Monitor**.
- **Admin Status:** To disable the admin status, check this check box and click **Disable**.
- **Power Assignment:** To choose a custom power value, check this check box and click **Custom**. Choose the power level from the **Select Custom Power** drop-down list.
- **Channel Assignment:** To choose custom channel numbers, check this check box and click the **Custom** button. Choose a custom channel number from the **Select Custom Channel** drop-down list.
- **Channel Width:** To choose channel width, check this check box and choose channel width.

Note Cisco DNA Center enables this parameter when you choose the **Custom** option for **Channel Assignment**.

- **CleanAir / Spectrum Intelligence:** To disable CleanAir spectrum intelligence, check this check box and click **Disable**.

Note You can configure CleanAir spectrum intelligence only on the CleanAir spectrum intelligence-capable APs that are in the **Local/FlexConnect** and **Monitor** modes. If the CleanAir spectrum intelligence is disabled on the 802.11a network, the operation state is down for the AP.

- **Antenna Gain:** To choose an antenna gain, check this check box and choose an antenna from the **Select Antenna** drop-down list. If you choose **Other** as the antenna, enter the antenna gain value in the **Antenna Gain (in dBi) (for Antenna-Other)** field. Enter a number to specify the ability of an external antenna to direct or focus radio energy over a region. High-gain antennas have a more focused radiation pattern in a specific direction. The antenna gain value range is from 0 through 40.

Note The selected antenna name isn't reflected in wireless maps.

- **Antenna Cable:** To choose an antenna cable, check this check box and choose the antenna cable from the **Select Antenna Cable** drop-down list. If you choose **Other** as the antenna cable, enter the cable loss value in the **Cable Loss (in dBi) (for Cable-Other)** field. The cable loss value is from 0 through 40.

Note Effective with Cisco DNA Center Release 2.3.5.3, the **Azimuth** and **Elevation** parameters are no longer available in the **Configure Access Points** workflow. You can configure the azimuth and elevation in the **Design > Network Hierarchy** window. For more information, see [Edit an AP, on page 152](#).

- Step 12** In the **Schedule Task** window, click **Now** or **Later** to indicate when you want to provision the AP.
- Step 13** In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)
- Step 14** Click **Configure**.
- Step 15** In the **Track Provision Status** window, view the **AP Configuration Provision** status.

Schedule Recurring Events for AP Workflow

This procedure shows how to schedule recurring events for AP and radio parameters in Cisco DNA Center.

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Configure Access Points**.
- Step 2** If an **Overview** window opens, click **Let's Do it** to start the workflow.
- Step 3** In the **Get Started** window, enter a unique name for the task in the **Task Name** field.
- Step 4** In the **How do you want to configure APs?** window, click the **Schedule Recurring Events For AP And Radio Parameters** radio button.
- Step 5** In the **Select Access Points** window, do the following:
- a) Navigate to the site where you want to apply AP-related configurations.
The right pane lists all the APs available in the selected site.
 - b) Check the check boxes next to the names of the AP that you want to configure.
- Step 6** In the **Select AP and Radio Parameters** window, choose the AP and radio parameters that you want to configure. Cisco DNA Center applies certain settings to only one of the AP slots, as follows:
- **5 GHz Admin Status:** Applied to slot 1 of the AP.
 - **2.4 GHz Admin Status:** Applied to slot 0 of the AP.
 - **6 GHz Admin Status:** Applied to slot 3 of the 6 GHz-capable Cisco Catalyst 9136 Series APs and slot 2 of the 6 GHz-capable Cisco Catalyst 9164 Series APs.
 - **Dual-Band (XOR) Admin Status:** Applied to slot 0 of the following dual-band (XOR)-capable APs:
 - Cisco Aironet 2800 Series Access Points
 - Cisco Aironet 3800 Series Access Points
 - Cisco Aironet 4800 Series Access Points
 - Cisco Catalyst 9120 Series Access Points

Applied to slot 2 of the dual-band (XOR)-capable Cisco Catalyst 9166 Series APs.

- **Tri-Radio Admin Status:** Applied to slot 2 of the tri-radio-capable APs with dual radio mode enabled.

To disable the configuration of a parameter, check the corresponding check box and click **Disable**.

Step 7 In the **Schedule Provision** window, configure the following:

- a. Specify the start date and time.
- b. Choose a time zone.
- c. For the **Recurrence** setting, click one of the following toggle buttons to indicate when Cisco DNA Center runs the AP configuration task:
 - **None:** Runs once and doesn't repeat.
 - **Hourly:** Cisco DNA Center runs the AP configuration task at every specified hour interval. In the **Run at Interval (Hours)** field, specify the interval, in number of hours, to repeat the task. The valid range is from 1 through 48.
 - **Daily:** Runs the AP configuration task at every specified day interval. In the **Run at Interval (Days)** field, specify the interval, in number of days, to repeat the task. The valid range is from 1 through 14.
 - **Weekly:** Runs the AP configuration task at every specified week interval. In the **Run at Interval (Weeks)** field, specify the interval, in weeks, to repeat the task. The valid range is from 1 through 52.
- d. (Optional) If you choose **Hourly**, **Daily**, or **Weekly** recurrence interval, check the **Set Schedule End** check box to complete the recurrence end settings:
 - To specify an end date, click the **End Date** radio button and specify the end date.
Note Cisco DNA Center allows a maximum end date of 3 years from the start date.
 - To end the recurring event after a specified number of occurrences, click the **End After** radio button and specify the number of occurrences.
Note Cisco DNA Center allows a minimum value of 2 and maximum end date of three years from the start date.

Step 8 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 9 Click **Configure**.

Learn Device Configurations from Devices with Pre-Existing Infrastructure

The following procedure shows how to learn configuration from devices with pre-existing infrastructure using Cisco DNA Center.

Step 1 Click the menu icon (☰) and choose **Workflows > Learn Device Configuration > Let's Do it** to launch the workflow.

Note At the top of the workflow window, place your cursor over the blue progress bar to know the current step you are on and also to switch back to any of the previous steps.

Step 2 In the **Select a WLC to Learn Configuration** window, click on the wireless controller whose configurations have not been learned by Cisco DNA Center and click **Next**.

Step 3 In the **Site Assignment** window, select sites that aren't associated with the existing wireless network profiles for wireless controllers and APs.

Note While you can learn device configuration without site assignment, we recommend that you assign sites, which is required to manage the same wireless controller from Cisco DNA Center.

- a) To assign a site to a wireless controller, click **Assign Site** next to the **Device Name**.
 - In the **Assign Site** window, navigate to the building that you want to associate and click **Save**.
- b) To assign sites to an AP, check the check box next to the AP name in the **Unified APs** table and click **Assign Site**.
 - In the **Assign Site** window, navigate to the floor and click **Save**.
- c) Click **Next**.

Step 4 In the **Learned Network Settings** window, review the following learned network settings.

These settings are saved to the physical location of the device. The network servers that are displayed in this window are saved at the site level.

- Enter the **Shared Secret** for AAA servers.

- **System Settings**

- To save a AAA server as a Cisco ISE server, click the **Cisco ISE Server** toggle button and enter the **Username**, **Password**, and **FQDN** details.

Note If the Cisco ISE server is already present on Cisco DNA Center, you cannot save a AAA server as a Cisco ISE server.

After configuring a AAA server as a Cisco ISE server, the certificate from the Cisco ISE server is automatically accepted to establish the trust.

- Click the **Virtual IP Address(es)** toggle button to enter the load balancer IP address.
- **AAA Server**: Shows the network servers configured on Cisco DNA Center. These network servers are prepopulated.
 - You can customize **Network** or **Client/Endpoint** for the AAA server. The servers and protocols are chosen by default.
 - From the drop-down list, choose **IP Address (Primary)** and **IP Address (Secondary)**. These servers are saved at the global level.
 - **DHCP Server**: Shows all the DHCP servers available on the device.
 - **NTP Server**: Shows all the NTP servers available on the device.
- Click **Next**.

- Step 5** In the **Assign Sites to Configurations Learned** window, you can view the following learned configurations if the configuration is available on the device. The configurations that aren't assigned to sites are ignored.
- Flex Override
 - AAA Server
 - VLAN Entry
 - Mesh Configuration
 - Enable Remote Teleworker
- Step 6** In the **Learned Wireless Configuration** window, review the configurations learned from the wireless controller. The wireless configurations that appear in this window are saved at the global level.
- The **Supported** tab shows the list of learned configurations, such as **SSID, RF Profiles, Interfaces, Interface Groups, aWIPS and Forensic Capture Enablement, Pre Auth ACLs, and VLAN**.
 - By default, the NAC configuration enabled SSIDs are learned as guest SSID. Click the **Edit** icon next to the **SSID Type** in the **SSIDs** table to change the SSID type from Guest to Enterprise.
 - To ignore the configuration, check the check box next to the learned configuration, and click **Ignore Config** in the corresponding table.
 - To relearn an ignored SSID, RF profile, interface, or interface group, select it and click **Relearn Config** in the corresponding table.
 - The **Unsupported** tab shows the configurations that are not learned, such as **SSIDs, RF Profiles, Interfaces, Pre Auth ACLs, and Interface Groups**. You can address these unsupported or unknown configurations and use CLI templates.
- Step 7** In the **Assign Sites to Learned SSIDs** window, review and resolve any multiple WLAN profile conflicts.
- The SSIDs that are saved at the global level and learned with multiple WLAN profiles are listed. You can assign a WLAN profile from each SSID to global and another profile to a particular site to resolve the conflict.
 - (Optional) To assign a WLAN profile to a site, click **Assign Site** in the corresponding SSID row.
 - In the **Assign Site** window, choose a site and click **Save**
- Note** Only the sites that do not have any wireless configurations or profiles that are associated to them can be overwritten. If there is no fresh site, exit from the current workflow, create a new site, and then restart the workflow.
- Step 8** In the **Resolve Configuration Conflicts** window, review and resolve the available conflicts. Configurations learned from the device and the configurations saved at the global level are shown. Choose a configuration set to resolve the conflict:
- **Use DNAC Configuration:** To save configurations at the global level.
 - **Use Device Configuration:** To learn configurations from the device.
Selecting device configuration overwrites the configurations saved at the global level.
 - **Use Custom Configuration:** To customize the configurations by choosing the required **Wireless Interface**.

Step 9 In the **Model Configs Learned** window, review the model configuration.

The model configurations are a set of model-based, discoverable, and customizable configuration capabilities that can be deployed on network devices. Model configurations can be deployed on various hardware platforms and software types. Cisco DNA Center discovers and learns model configs from device-specific configurations such as CLI. The learned model configs are saved in designs that can be attached to network profiles.

Expand and review the following wireless model config design types:

- AAA Radius Attributes Configuration
- Advanced SSID Configuration
- CleanAir Configuration
- Dot11ax Configuration
- Event Driven RRM Configuration
- Global IPv6 Configuration
- Multicast Configuration
- RRM General Configuration

If you want to ignore any configuration from each model configuration design type, select the configuration in the corresponding table and click **Ignore Config**. To relearn the ignored configuration, select the ignored configuration and click **Relearn Config**.

Step 10 In the **CLI Templates Learned** window, review the CLI templates and use these templates to address the unknown or unsupported configurations.

- All the ignored WLAN configs are chosen by default. Click **Ignore Template** to restrict the template from addressing the configs. Click **Relearn Template** to address the configs.
- All the unknown or unsupported configs are chosen by default. Click **Ignore Template** to restrict the template from addressing the configs. Click **Relearn Template** to address the configs.

Step 11 In the **Network Profiles** window, review the learned network profile configuration. Based on the configurations learned, Cisco DNA Center creates the network profile. You can either use the learned network profile or create a new network profile. The SSIDs are learned and grouped while creating network profile.

For Cisco AireOS Wireless Controllers, the Flex group and AP groups are mapped to the network profile. Depending on the AP site assignment, the network profile is assigned to the appropriate site.

For Cisco Catalyst 9800 Series Wireless Controllers, the site tag, policy tag, and site hierarchy that is mapped to the network profile is displayed.

- Based on the AP site assignment configuration, network profile is assigned to the appropriate site. Click **Sites Assigned** to view details on the site assigned to the network profile.
- To create a new network profile, click **Create New Profile**.

The **New Profile** window appears.

- In the **Network Profile Name** field, enter a name for the network profile.
- From the **SSIDs** table, check the check box next to the **Network Name** to select the SSID.
- Click **Save**.

- (Optional) Review the template details and edit if you want to make any changes.
 - To assign a site to a network profile, click **Assign Site**. In the **Assign Site** window, choose a site and click **Save**.
Click **Sites Assigned** to view the sites assigned to this profile.
 - To attach a template to a network profile, click **Assign Template**. In the **Assign Template** window, choose templates from the **Select Templates** drop-down list for each device in the existing deployment and click **Save**.
Click **View Templates** to view the templates assigned to the profile.
 - To ignore a network profile, click **Ignore Profile** and click **Continue**.
If a profile is marked as ignored, all the profile attributes of that profile are removed. This cannot be undone by relearning the profile. To relearn an ignored profile, click **Relearn Profile**.
 - To add a site tag to a network profile, click **Add** in the **Site Tag** table. In the **Add Site Tag** window, choose a site tag from the **Select Site Tag** drop-down list, choose a site from the hierarchy, and click **Save**.

Step 12 (Optional) In the **Network Profile - Model Configurations** window, associate model configurations learned by Cisco DNA Center into the network profiles.

- Click **Add**.
- In the **Add Model Configs to Network Profile** window, do the following:
 - Expand the model config design that you want to add.
 - Choose the design. For **Advanced SSID Configuration**, for each design, choose SSIDs from the drop-down list in the **Applicable SSID** column.
 - Click **Apply**.
- To delete a model config added to the network profile, choose the model config and click **Delete**.
- Click **Next**.

Step 13 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 14 Click **Save**.

The network configurations are created at the global and site level appropriately.

Step 15 Click the menu icon (☰) and choose **Design > Network Settings**.

- In the **Network** tab, you can view all the network configurations learned from devices.
- In the **Wireless** tab, you can view all the wireless configurations learned from devices.

The learned configurations are pushed to devices when the devices are provisioned.

Replace Device Workflow

The workflow guides you step by step to replace a faulty device.

For Cisco Switch stacks (hardware stacking), you do not need to follow a separate procedure in Cisco DNA Center for member switch replacement, it is handled by the active switch. The member switch is replaced by the active switch by providing software image and configuration. Full stack replacement is handled by Cisco DNA Center.



Note You can also replace a faulty device from the **Inventory** window. For more details, see [Replace a Faulty Device](#), on page 109.

Before you begin

- The software image version of the faulty device must be imported in the image repository before marking the device for replacement.
- The faulty device must be in an unreachable state.
- The faulty device must be assigned to a user-defined site, if the replacement device onboards Cisco DNA Center through Plug and Play (PnP).
- The replacement device must not be in a provisioning state while triggering the RMA workflow.
- For switch stacks replacement, the number of stacks for faulty and replacement device should be same.

-
- Step 1** Click the menu icon (☰) and choose **Workflows > Replace Device**.
- Step 2** If a task overview window opens, click **Let's Do it** to go directly to the workflow.
- Step 3** In the **Get started** window, enter a unique **Task Name** for your workflow.
- Step 4** In the **Choose Device Type** window, choose the type of faulty device that you want to replace.
- Step 5** In the **Choose Site** window, choose the site in which you have the faulty device.
- Step 6** In the **Choose Faulty Device** window, choose one faulty device that you want to replace.
- Step 7** In the **Choose Faulty Device** window, if you don't find the faulty device, do the following:
- a) Click **Add Faulty Device**.
 - b) Choose the faulty device and click **Next**.
 - c) In the **Mark for Replacement** window, click **Mark**.
- Step 8** In the **Choose Replacement Device** window, choose a replacement device from the **Unclaimed** tab or **Managed** tab.
- The **Unclaimed** tab shows the devices that are onboarded through PnP. The **Managed** tab shows the devices that are onboarded either through Inventory or the discovery process.
- Step 9** (Optional) If the replacement device is not yet onboarded, do the following:
- a) In the **Choose Replacement Device** window, click **Add Device**.
 - b) In the **Add New Device** window, enter the **Serial Number** of the device and click **Add New Device**.
- Or

- a) In the **Choose Replacement Device** window, click **Sync with Smart Account**.
- b) In the **Sync with Smart Account** window, click **Sync**.

Step 10 In the **Schedule Replacement** window, click **Now** to start device replacement immediately or click **Later** to schedule device replacement at a specific time.

If the replacement device is not yet onboarded, the **Now** option is disabled. Click **Later** to schedule the device replacement at a specific time.

Step 11 Click **Review** to view the chosen device type, faulty device details, and replacement device details.

Step 12 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

- a) (Optional) Under **Replacement Device**, click **View** to view the configuration of the replacement device.
- b) Click **Replace**.

Step 13 Click **Monitor Replacement Status** to go to the **Mark for Replacement** view in the **Provision** window.

Step 14 Click **Replace Status** to view the status of the RMA workflow progress, as follows:

- Running readiness checks for device replacement.
- Claim the (PnP) replacement device.
- Distribute and activate the software image to the replacement device.
- Deploy licenses.
- Provision VLAN configurations.
- Provision startup configurations.
- Reload the replacement device.
- Check for reachability of the replacement device.
- Deploy SNMPv3 credentials to the replacement device.
- Synchronize the replacement device.
- Remove the faulty device from CSSM.
- Add the replacement device to CSSM.
- Revoke and create the PKI certificate.
- Update Cisco ISE.
- Delete the faulty device.

After the workflow is completed, the **Replace Status** is updated to **Replaced**.

Step 15 If an error message appears, click the error link. Click **Retry** to retrigger the workflow with the same set of faulty and replacement devices.

Note The main inventory window displays the details of the new replacement device that has replaced the faulty device.

Step 16 (Optional) You can exit the workflow at any stage and resume it later. The Exit option is shown at the bottom left corner in all the windows. To exit the workflow and resume it later, do the following:

- a) Click **Exit**.

The **Exiting Workflow** confirmation window appears.

- b) Click **Exit** in the confirmation window.

A workflow **In Progress** card with the task name is created.

- c) To resume the work flow from where you left, click the **In Progress** card.

- If a device has **In progress** card and you try to replace the same device from **Inventory > Marked for Replacement** window, a confirmation message with the serial number and task name of **In progress** card appears. Click **Yes** to resume the work-flow or **Cancel** to start a new workflow.
- If you click the **In progress** card for a device that is unmarked for replacement, a **Warning message** appears. Click **Yes** and choose a different faulty device to start a new workflow. If you click **Cancel** the workflow will be cancelled.

Create a Remote Support Authorization

The following procedure describes how to create a remote support authorization.



Note The Cisco DNA Center remote support authorization is supported only with RADKit version 1.2.1 or later.

Step 1 Click the menu icon (☰) and choose **Workflows > Create a Remote Support Authorization**.

Step 2 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Set up the Authorization** window, enter the following:

- a) **Cisco Specialist Email Address**
- b) **Existing SR Number(s)**
- c) **Access Justification**

Step 4 In the **Schedule the Access** window, click **Now** or **Later** to indicate when you want to allow the Cisco specialist to access Cisco DNA Center.

Step 5 In the **Access Permission Agreement** window, do the following:

- a. Check the **I agree to provide access to network devices** check box to provide access to network devices.
- b. Check the **I agree to provide access to our Cisco DNA Center setup** check box to allow a Cisco specialist to access your Cisco DNA Center setup using SSH credentials.

- Note**
- You must create the SSH credentials before completing a remote support authorization. To create SSH credentials, see [Configure SSH Credentials](#).
 - You can cancel or revoke the authorization at any time before the access. To cancel the authorization, see [View the Remote Support Authorization Dashboard](#).

Step 6 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 7 Click **Create**.

The **Done! Authorization is created** window appears.

Step 8 Click **View All Authorizations** to navigate to the **Remote Support Authorization** window. For information, see [View the Remote Support Authorization Dashboard](#).

Create an Event Notification

Cisco DNA Center event notification allows you to associate multiple channels inside one notification that delivers the details of selected events that occur at multiple points.

Step 1 Click the menu icon (☰) and choose **Workflows > Create a New Notification**.

Step 2 If a task overview window opens, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Select Channels** window, choose the notification channels.

The supported channels are **REST**, **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, **EMAIL**, and custom channels. Assurance events do not support SNMP.

Step 4 In the **Select Site and Events** window, from the **Select a site** drop-down list, choose a specific site for which you want to be notified for the selected events.

Note You can choose multiple sites at a time.

Step 5 Click either the plus icon next to an event, or click **Add All** to add all the events to the respective notification.

Step 6 To remove an event from the notification, click either the cross icon next to the event that you want to remove, or click **Remove All** to remove all the event from the event list.

Note

- When you choose a notification channel, a table in the **Select Site and Events** window lists the number of events supported by the chosen notification channel.
- When you choose more than one notification channel, a table in the **Select Site and Events** window lists the number of supported events that are common in the chosen notification channels.

Step 7 In the **Configure Notification** window, configure the following values:

a. If you choose an **EMAIL** notification channel, configure the following in the **Email Settings** window:

1. Click the link to access the Email GUI window and configure a new email server.


- Note**
- Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you choose **EMAIL**, but have not yet configured the email settings, you are prompted to access the GUI window where you can perform this task. Email settings are configured in the **Email** tab.

(Optional) To access the **Email** tab, click the menu icon (≡) and choose **System > Settings > External Services**.

Expand **External Services**, choose **Destinations**, and click the **Email** tab.

- Up to 20 email addresses per endpoint can be configured to receive email notifications. To add multiple email addresses, you need to add each email address separately and press **Enter** (on your keyboard) after each addition. Cisco DNA Center validates the email addresses and notifies you if the syntax is incorrect.
 - If you need to configure more than 20 email addresses per endpoint, you can use a group email alias.
 - When using email destinations for event subscriptions, the emails that are sent show events with a UTC timestamp.
- Click either **Select Existing Instance** to use the existing email instance or **Create New Instance** to create a new email instance.
 - If you click **Select Existing Instance**, from the **Select Instance** drop-down list, choose an email instance.
 - Enter the email addresses in the **From** and **To** fields and a subject for the **Subject** header in the email.
- b.** If you choose a **SYSLOG** notification, configure the following values in the **Syslog Settings** window:
- Click the link to access the Syslog GUI window and configure a new syslog endpoint (syslog server hostname and port number).
- Note**
- Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you choose **SYSLOG**, but have not yet configured the syslog server settings, you are prompted to access the GUI window where you can perform this task. Syslog server settings are configured in the **Syslog** tab.
- (Optional) To access the **Syslog** tab, click the menu icon (≡) and choose **System > Settings > External Services**.
- Expand **External Services**, choose **Destinations**, and click the **Syslog** tab.
- In the **Protocol** field, enter either TCP or UDP.
 - In the **Port** field, enter the port number of the syslog server.
 - In the **Hostname/IP** field, enter the hostname or IP address of the syslog server.
 - From the **Select Instance** drop-down list, choose the syslog instance.
- c.** If you choose a **REST** notification, configure the following values in the **REST Settings** window:
- Click the link to access the REST Webhook GUI window and configure a new webhook endpoint.

Note Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you select **REST**, but have not yet configured the webhook settings, you are prompted to access the GUI window where you can perform this task. Webhook settings are configured in the **Webhook** tab.

(Optional) To access the **Webhook** tab, click the menu icon () and choose **System > Settings > External Services**.

Expand **External Services**, choose **Destinations**, and click the **Webhook** tab.

- From the **Webhook Instance** drop-down list, choose a notification endpoint and URL.
- In the **URL** field, enter the URL address of the REST API endpoint that the event will be sent to.

Trust certificate: Whether a trust certificate is required for REST API endpoint notification.

Method: Either the PUT or POST method.


- **Basic:** Authentication where the client sends HTTP requests with the word *Basic* in the authorization header, followed by a space and a base64-encoded string username:password. If you choose **Basic** in the GUI, the **Headers** field is automatically populated with the **Authorization** value.
- **Token:** Authentication where users are authenticated using a security token provided by the server. If you choose **Token**, the **Headers** field is automatically populated with the **X-Auth-Token** value.
- **No Authentication:** No authentication needed.
- **Headers:** The **Header Name** and **Header Value**.

Note The **Headers** fields may be automatically populated depending on your Authentication selection.

d. If you choose **SNMP** notification channel, configure the following values in the **SNMP Settings** window:

1. Click the link to access the SNMP GUI window and configure a new SNMP endpoint.

Note Notification type can be set for either **REST** API endpoint (webhook), **PAGERDUTY**, **SNMP**, **SYSLOG**, **WEBEX**, and **EMAIL**. If you select **SNMP**, but have not yet configured the SNMP settings, you are prompted to access the GUI window where you can perform this task. SNMP settings are configured in the **SNMP** tab.

(Optional) To access the **SNMP** tab, click the menu icon () and choose **System > Settings > External Services**.

Expand **External Services**, choose **Destinations**, and click the **SNMP** tab.

The SNMP trap notification is only available for a system hardware event. When the health state of hardware components changes, a system hardware event triggers notifications to subscribers. Hardware components monitored for changes include CPU, memory, disk, NIC, fan, power supply, and RAID controller.

2. From the **SNMP Instance** drop-down list, choose the notification endpoint.
3. **Create a new endpoint:** Enter a new endpoint name and description.
4. In the **Hostname/IP Address** field, enter the hostname or IP address for the SNMP trap receiver (server).
5. In the **Port** field, enter the port number for the SNMP trap receiver (server).

- e. If you choose **PAGERDUTY** notification channel, configure the following in the **PAGERDUTY settings** window:
 1. In the **SERVICE CONFIGURATION** area, click either **Select Existing Instance** to use the existing PagerDuty instance or **Create New Instance** to create a new PagerDuty instance.
 2. From the **Select Instance** drop-down list, choose a PagerDuty instance.
 3. In the **PagerDuty Events API URL** field, enter a PagerDuty event API URL.
 4. In the **PagerDuty Integration Key** field, enter a PagerDuty integration key.
- f. If you choose **WEBEX** notification channel, configure the following values in the **WEBEX Settings** window:
 1. From the **Select Instance** drop-down list, choose a Webex instance.
 2. In the **Webex URL** field, enter the Webex URL.
 3. In the **Webex Room ID** field, enter the Webex room ID.
 4. In the **Webex Bot Access Token** field, enter the Webex bot access token.

Step 8 Click **Save**.

In the **Name and Description** window, do the following:

- a) In the **Name** field, enter a unique name for the notification.
- b) In the **Description** box, enter a description of the notification.

Step 9 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 10 Click **Finish**.

The **Done! Your new notification is complete** window appears.

Configure Remote LAN

Remote LAN (RLAN) allows you to configure RLAN ports on APs for Cisco Wireless Controller. Wireless controller authenticates the wired clients and allows them to connect to the network.

Cisco DNA Center supports RLAN configuration only on Cisco Catalyst 9800 Series Wireless Controller. You can configure RLAN for nonfabric sites on wireless controllers that run Cisco IOS XE Release 16.12 or later. You can configure RLAN for fabric sites on wireless controllers that run Cisco IOS XE Release 17.7 or later.



Note Cisco DNA Center doesn't support RLAN configuration on Cisco AireOS Wireless Controllers.

This section provides information about how to configure RLAN ports.

Before you begin

- Ensure that you have provisioned a Cisco Wireless Controller and at least one AP for the site.

To configure RLAN ports for fabric sites:

- Ensure that you have provisioned the required fabric site.
- Ensure that you have created IP pools and Security Group Tags (SGT).

Step 1 Click the menu icon (☰) and choose **Workflows > Configure RLAN**.

Step 2 If a task overview window appears, click **Let's Do It** to go directly to the workflow.

Step 3 In the **Get Started** window, enter a unique name for the task.

Step 4 In the **Select Floor** window, navigate to the floor where you want to configure RLAN ports.

The right pane shows the summary for the selected floor. Cisco DNA Center configures RLAN for all the APs provisioned on the selected floor.

Step 5 In the **Remote LAN Configuration** window, do the following:

a) Choose the required RLAN port from the **Port 1**, **Port 2**, and **Port 3** options.

If the AP has a single RLAN port, Cisco DNA Center ignores the **Port 2** and **Port 3** configurations for the AP.

b) Click the **Enable RLAN** toggle button to enable or disable RLAN.

c) In the **Connectivity Settings** area, click the **Fabric** toggle button to configure RLAN ports for a fabric or nonfabric site.

Note After you configure the connectivity settings for fabric or nonfabric, you can't modify the option later.

If you enable the **Fabric** toggle button, do the following:

- In the **IP Address Pool** field, enter the IP address.
- (Optional) From the **Scalable Group Tag** drop-down list, choose the required option.

If you disable the **Fabric** toggle button, do the following:

- From the **Select Switching** drop-down list, choose the required option.
- In the **VLAN** field, enter the VLAN number. The valid range for VLAN is from 1 through 4096.

d) In the **Security Settings** area, do the following:

- In the **Maximum End Points** field, enter the number of endpoints. The valid range is from 0 through 10000.

Note This field configures the client connections per RLAN. 0 indicates unlimited client connections.

- In the **Timeout Period (in seconds)** field, enter the timeout period, in seconds. The valid range for timeout is from 0 through 86400.

- (Optional) From the **Layer 2** drop-down list, choose the required option.

- (Optional) To enable MAC filtering, check the **MAC Filtering** check box.

- (Optional) From the **Fallback Authentication** drop-down list, choose the required option.

Note Fallback mechanism is supported on both fabric and nonfabric sites on Cisco Catalyst 9800 Series Wireless Controllers that run Cisco IOS XE Release 17.8 or later.

- (Optional) From the **Layer 3** drop-down list, choose the required option.
- (Optional) From the **Select a AAA Server Group** drop-down list, choose an AAA server group.

This drop-down list provides the list of AAA server groups configured as part of WLAN provisioning on the primary controller. If you don't choose an AAA server group, Cisco DNA Center configures the default method under the RLAN profile for the selected security settings.

- e) (Optional) In the **Point over Ethernet Settings** area, use the **PoE** toggle button to enable or disable the Point over Ethernet (PoE).

Note Cisco DNA Center enables PoE only on APs with PoE-capable ports.

Step 6 In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.

Step 7 In the **Schedule Task** window, do one of the following:

- Click **Now** or **Later** to indicate when you want to provision.
- Click **Generate Preview** to create a preview that you can use later to deploy the settings on selected devices.

Step 8 Click **Apply**.

What to do next

You can view the status of the RLAN configuration in the **Activities > Tasks** window.

If you have provisioned a secondary wireless controller, reprovision the secondary wireless controller from the **Provision > Inventory** window.

Workflow to Create an IP- and URL-Based Access Control Policy

You can create a post authentication access control list (ACL) for your network. The ACL can be based on IPs, URLs, or both.

Before you begin

[Create an IP-Based Access Control Contract, on page 585](#)

Step 1 Click the menu icon (☰) and choose **Workflows > Create IP & URL-Based Access Control Policy**.

Note If an **Overview** window opens, click **Let's Do it** to start the workflow.

Step 2 In the **Policy Name and Details** window:

- a) Enter a name and description for the policy.
- b) Under **Select ACL Type**, check the **IP** check box, the **URL** check box, or check both the **IP** and **URL** check boxes.

Step 3 In the **Select Site and SSID** window, choose the site where you want to apply the policy.

Make sure the site is already provisioned with a nonfabric SSID.

Step 4 If you selected the **IP** check box in the **Policy Name and Details** window, do the following in the **IP Access Control List** window:

- a) Click **Add New Row** and choose **Source**, **Destination**, **Contracts**, or **Direction**.
- b) Click **Add**.

Step 5 If you selected the **URL** check box in the **Policy Name and Details** window, do the following in the **URL Access Control List** window:

- a. Enter the URL.
- b. Click the **Actions** drop-down list and choose **Permit** or **Deny**.

Step 6 In the **Schedule Task** window, do one of the following:

- To proceed with the deployment, choose either the **Now** or **Later** radio button.
- To create a preview that you can deploy later on selected devices, click the **Generate Preview** radio button.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8 Click **Deploy**.



CHAPTER 32

Troubleshoot Cisco DNA Center Using Data Platform

- [About Data Platform, on page 739](#)
- [Troubleshoot Using the Analytics Ops Center, on page 740](#)
- [View or Update Collector Configuration Information, on page 741](#)
- [View Data Retention Settings, on page 742](#)
- [View Pipeline Status, on page 743](#)

About Data Platform

Data Platform provides tools that can help you monitor and troubleshoot Cisco DNA Center applications. **Data Platform** displays synthesized data from various inputs to help you identify patterns, trends, and problem areas in your network. For example, if something goes wrong in your network, you can quickly get answers to questions such as whether a pipeline is in an error state and what is the real-time traffic flow in a particular area. The main areas of Data Platform are:

- **Analytics Ops Center:** Provides a graphical representation of how data is streamed through collectors and pipelines and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network. See [Troubleshoot Using the Analytics Ops Center, on page 740](#).
- **Collectors:** Collects a variety of network telemetry and contextual data in real time. As data is ingested, Cisco DNA Center correlates and analysis the data. You can view the status of collectors and quickly identify any problem areas. See [View or Update Collector Configuration Information, on page 741](#).
- **Store Settings:** Allows you to view how long data is stored for an application. See [View Data Retention Settings, on page 742](#).
- **Pipelines:** Allows Cisco DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas. See [View Pipeline Status, on page 743](#).

Troubleshoot Using the Analytics Ops Center

The Analytics Ops Center provides a graphical representation of how data is streamed through collectors and pipelines, and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network, such as:

- Missing data in Assurance.
- An inaccurate health score.
- Devices that appear as monitored under Inventory but unmonitored under Assurance.

Step 1 Click the menu icon (☰) and choose **System > Data Platform**.

Step 2 Click **Analytics Ops Center**.
A list of applications is displayed.

Step 3 Click the application name for which you want to view metrics; for example, **Assurance**.

A graphical representation of all existing collectors and pipelines in the application appears. CPU or throughput values corresponding to each pipeline are also provided.

The current health status of each component is indicated by its color:

- Red: error
- Yellow: warning
- Gray: normal operation

Step 4 To view historical data of pipelines, click **Timeline & Events**.

A timeline bar providing data for the time interval appears. You can also:

- Move the timeline slider to view data for a specific time.
- Hover your cursor over an event in the timeline bar to display additional details or a group of events that occurred at the same time.
- Click an event to display the Analytics Ops Center visualization at that particular time.

Step 5 To view additional details to help you troubleshoot an issue and determine the cause of an error or warning, click a collector name.

A slide-in pane appears with the following tabs:

- **Metrics:** Provides a selection of available metrics gathered during the last 30 minutes. It displays summary information indicating the component status, start and stop time, and error exceptions. You can also choose a different time interval.
- **Grafana:** Displays a dashboard associated with the respective component for deeper debugging.

Step 6 To view whether data is flowing through a specific pipeline, click a pipeline stream.

A slide-in pane appears with graphs. The graphs display whether the application is receiving data from the underlying pipelines. The graph information is based on the time interval you select from the drop-down list in the slide-in pane. Options are **Last 30 Min**, **Last Hour**, **Last 2 Hours**, and **Last 6 Hours**. The default is **Last 30 Min**.

Step 7 If a pipeline is not flowing at normal levels, hover your cursor over the stream to display the lag metrics.

Step 8 To view detailed information for a specific pipeline, click a pipeline name.

The appropriate *Pipeline* page displays with the following tabs:

Note Make sure to click the **Exceptions** tab to determine if any exceptions occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics**: Displays metrics, updated every 30 minutes in a graph.
- **Summary**: Displays summary information such as stats, run-time, and manifest.
- **Exceptions**: Displays any exceptions that occurred on the pipeline.
- **Stages**: Displays the pipeline stages.

Step 9 To change the metrics displayed on the Analytics Ops Center page, click **Key Metrics**, select up to two metrics, and then click **Apply**.

By default, Cisco DNA Center displays CPU and Throughput metrics.

Step 10 To view metrics for a particular flow, do the following:

- a) Click **View Flow Details**.
- b) Select three connected components (collector, pipeline, and store) by clicking the tilde (~) on the component's top-left corner.
- c) Click **View Flow**.
Cisco DNA Center displays the metrics associated with that specific flow.

View or Update Collector Configuration Information

Collectors collect a variety of network telemetry and contextual data in real time. As data is ingested, Cisco DNA Center correlates and analyzes the data. You can view the status of collectors and quickly identify any problem areas.

Step 1 Click the menu icon (☰) and choose **System > Data Platform**.

Step 2 Click **Collectors**. The colored dot next to each collector indicates its overall status.

Step 3 To view additional details, click a collector name.

The appropriate *Collector* page appears. By default, Cisco DNA Center displays the **Configurations** tab which displays the list of current configurations.

Step 4 To view, update, or delete a configuration, click a specific configuration name.

Step 5 To add a new configuration, click + **Add** in the **Configurations** tab.

Step 6 In the slide-in pane, enter the required information for the configuration.

- Step 7** (Optional) For some collectors, such as the wireless collector, you can check the **Anonymize** check box to scramble the host name and user ID in the **Client Health** window with a one-way hash that cannot be decrypted.
- Important** If you want to anonymize your data, make sure that you check the **Anonymize** check box before you discover devices with the **Discovery** tool. If you anonymize the data after you discovered devices, the new data coming into the system is anonymized but the existing data will not be anonymized.
- Step 8** Click **Save Configuration**.
- Step 9** To view configured instances, click the **Instances** tab.
- Step 10** To view summary information and metrics, choose an instance from the list.
- Step 11** (Optional) If Cisco DNA Center integrates with Cisco Connected Mobile Experience (CMX), you have the option of anonymizing data on the CMX side. Do the following:
- Using an SSH client, log in to Cisco CMX as the `cmxadmin` CLI user.
 - Change to the root user.
 - Go to `/opt/cmx/etc/node.conf` and under `[location]`, add **user_options**. For example:


```
[location]
...
user_options=-Dhideusername=true
```
 - On the Cisco CMX CLI, enter the following commands:


```
cmxctl agent restart
cmxctl location restart
```
-

View Data Retention Settings

You can view how long data is stored for an application.

- Step 1** Click the menu icon (☰) and choose **System > Data Platform**.
- Step 2** Click **Store Settings**.
- Step 3** To view a list of historical purge jobs that have completed, click **Data Purge Schedule**.
The **HISTORY** table lists the name of the purge job, the result, time, and other data. You can sort, filter, and export data in the table.
- Step 4** To view the current data retention and purge settings, click **Data Retention & Purge Configuration**. The following is displayed:
- Document Store:** Settings for all time-based data, such as the maximum size and the low and high watermark threshold.
 - Metric Graph Store:** Settings for all time-based graphical data, such as the maximum size and the low and high watermark threshold.
-

View Pipeline Status

Data pipelines allow Cisco DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas.

Step 1 Click the menu icon (☰) and choose **System > Data Platform**.

Step 2 Click **Pipelines**.

Step 3 To view whether the application is receiving data from the underlying pipelines, click a pipeline name.

The appropriate *Pipeline* page displays with the following tabs:

Note Make sure to click the **Exceptions** tab to determine if any exceptions have occurred in the pipeline. Under normal working conditions, this tab displays **null**.

- **Metrics:** Displays metrics, updated every 30 minutes in a graph.
- **Summary:** Displays summary information such as stats, run-time, and manifest.
- **Exceptions:** Displays any exceptions that have occurred on the pipeline.
- **Stages:** Displays the pipeline stages.

