



## **Cisco Evolved Programmable Network Manager 2.2 User and Administrator Guide**

**First Published:** 2018-04-02

**Last Modified:** 2018-06-29

### **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

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/go/trademarks>. 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)

© 2018 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### PART I

---

#### Get Started with Cisco EPN Manager 33

### CHAPTER 1

#### Get Started With Cisco EPN Manager 1

Web Client Requirements 1

Log In and Out 2

Setup Tasks That Should Be Completed Before Using Cisco EPN Manager 2

Change Your Password 3

Use the Main Window Controls 3

Change Your Default Home Page 5

Set Up and Use the Dashboards 6

Types of Dashboards 6

Service Performance Dashboard Overview 7

Performance Dashboard Overview 8

Network Summary Dashboard Overview 12

Cable Dashboard Overview 15

Device Trends Dashboard Overview 17

DWDM/OTN Performance Dashboard Overview 18

How to Use the Dashboards 18

Add a New Dashboard 20

Customize a Dashboard Tab 20

Add Dashlets to Dashboards 21

Customize the Dock Window 23

Find Out Why Data Is Missing from a Dashboard 24

Work In a Different Virtual Domain 24

Manage Jobs Using the Jobs Dashboard 25

Extend Cisco EPN Manager Functions 26

[Check Cisco.com for the Latest Cisco EPN Manager Documentation](#) 27

---

## PART II

---

### **Manage the Inventory** 29

#### **CHAPTER 2**

### **Add and Organize Devices** 31

[Which Devices Are Supported by Cisco EPN Manager ?](#) 31

[Which Device Software Versions Are Supported by Cisco EPN Manager ?](#) 32

[How Is Inventory Collected?](#) 33

[Configure Devices So They Can Be Modeled and Monitored](#) 34

[Configure Devices To Forward Events To Cisco EPN Manager](#) 34

[Required Settings—Cisco IOS Device Operating System](#) 35

[Required Settings—Cisco IOS XE Device Operating System](#) 35

[Required Settings—Cisco IOS XR Device Operating System](#) 36

[Required Settings—Cisco NCS Series Devices](#) 37

[Required Settings—Cisco NCS 4000 Series Devices](#) 38

[Required Settings—Cisco NCS 4200 Series Devices](#) 40

[Required Settings—Cisco ONS Device Operating System](#) 42

[Required Configuration for IPv6 Devices](#) 42

[Apply Device Credentials Consistently Using Credential Profiles](#) 42

[Create a New Credential Profile](#) 43

[Apply a New or Changed Profile to Existing Devices](#) 43

[Delete a Credential Profile](#) 44

[Add Devices to Cisco EPN Manager](#) 44

[Add Cisco ME1200 devices in Cisco EPN Manager](#) 45

[Add Devices Using Discovery](#) 45

[Verify SNMP Communication](#) 46

[Specify the Management IP Address Type \(IPv4/IPv6\) for Discovered Devices](#) 46

[Run Quick Discovery](#) 47

[Run Discovery With Customized Discovery Settings](#) 47

[Import Devices Using a CSV File](#) 49

[Create the CSV File](#) 49

[Import the CSV File](#) 50

[Add Devices Manually \(New Device Type or Series\)](#) 50

[Example: Add a Single Cisco NCS 2000 or NCS 4000 Series Device](#) 51



Example: Add a Network Element as an ENE Using Proxy Settings	51
Check a Device's Reachability State and Admin Status	52
Device Reachability and Admin States	52
Move a Device To and From Maintenance State	53
Validate Added Devices and Troubleshoot Problems	54
Find Devices With Inventory Collection or Discovery Problems	55
Export Device Information to a CSV File	55
Create Groups of Devices for Easier Management and Configuration	55
How Groups Work	56
Network Device Groups	56
Port Groups	57
How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups	58
Groups and Virtual Domains	59
Create User-Defined Device Groups	59
Create Location Groups	60
Create Port Groups	61
Make Copies of Groups	61
Hide Groups That Do Not Have Any Members	62
Delete Groups	62
Delete Devices	62

---

## CHAPTER 3

<b>View Device Details</b>	<b>63</b>
Find Devices	63
Get Basic Device Information: Device 360 View	63
Compare Device Information and Status	66
View a Device's Local Topology from the Device 360 View	67
View the Network's Hardware Inventory	68
Get Complete Device Information: Device Details Page	68
Configure Interfaces from the Device Details Page	70
Update Cisco NCS 1000 Interface Settings	71
View and Manage Devices Using the Chassis View	72
Open the Chassis View	72
Permissions Required to View and Configure Devices Using the Chassis View	73
Overview of the Chassis View Window	73

Device Support for the Chassis View in this release of Cisco EPN Manager	76
View Network Element State Information in the Chassis View	78
Equipment Operational States (Chassis View)	78
Port or Interface States	78
View Mixed Chassis, Multi-Chassis, and Multi-Shelf Devices in the Chassis View	79
View Alarms in the Chassis View	80
View Device Ports	82
View Device Interfaces	82
View a Specific Device's Interfaces: Device 360 View	83
Get a Quick Look at a Device Interface: Interface 360 View	83
Compare Interface Information and Status	84
Get Comprehensive Information About a Device's Interfaces Using the Device Details Page	85
View Device Modules	86
View Environment Information (Power Supplies, Fans)	86
View Device Neighbors	87
Get More Information About Links	87
View Circuits/VCS	88
View Satellites	88
Create User Defined Fields for Custom Values	88

---

**CHAPTER 4**
**Manage Device Configuration Files 91**

Set Up Device Configuration File Management	91
Make Sure Devices Are Configured Correctly	91
Control How Archiving is Triggered	92
Set Up Event-Triggered Archiving	92
Specify Items to Be Excluded When Configuration Files Are Checked for Changes	93
Control the Timeouts for Configuration Archive Operations	93
Control How Often Alarms are Triggered	93
Control How Often the Archive Summary Is Updated	94
Control How Many Files Can Be Archived In Parallel	94
Control Whether Configuration File Content Is Masked During Exports	94
Control When Device Configuration Files are Purged from the Database	94
How Do I Find Out the Last Time Files Were Archived?	95
Back Up Device Configuration Files to the Archive	95

What Is Backed Up to the Database?	95
Back Up (Archive) Configuration Files	96
View the Device Configuration Files That Are Saved in the Archive	97
View All Archived Files	97
View Archived Files for a Specific Device	98
View the Raw Content of an Archived Configuration File	98
View a Device's Running Configuration File (Raw Content)	99
Label Important Configuration Files With Tags	99
Synchronize Running and Startup Device Configurations	99
Download Configuration Files	100
Compare or Delete Device Configuration Files	100
Deploy an External Configuration File to a Device	101
Overwrite a Startup Configuration with a Running Configuration	102
Roll Back a Device's Configuration To an Archived Version	102
Export Configuration Files to a Local File System	104
Delete Archived Device Configuration Files	104
Check the Network Audit for Configuration Archive Operations	105

---

## CHAPTER 5

### Manage Device Software Images 107

Set Up Software Image Management	107
Make Sure Devices Are Configured Correctly	108
Verify the FTP/TFTP/SFTP/SCP Settings on the Cisco EPN Manager Server	108
How to Control Images that are Saved to the Image Repository During Inventory Collection	108
Adjust Criteria for Cisco.com Image Recommendations	109
Adjust Image Transfer and Distribution Preferences	109
Add a Software Image Management Server to Manage Groups of Devices	110
Change Cisco.com Credentials for Software Image Operations	111
Copy Software Images from Devices to the Image Repository (Create a Baseline)	111
How Do I Find Out Which Images Are Used by Network Devices?	111
How Do I Know a Device Has the Latest Image?	112
View the Images That Are Saved in the Image Repository	112
Find Out Which Devices Are Using an Image	113
View Recommended and Available Software Images from Cisco.com	113
View Recommended Images on Cisco.com	113

View Available Images on Cisco.com	114
How Do I Know Whether I have Permission to Download Software from Cisco.com	115
Add (Import) Software Images to the Repository	115
Add a Software Image That Is Running on a Managed Device	115
Add a Software Image from an IPv4 or IPv6 Server (URL)	116
Add a Software Image for an FTP Protocol Server (Protocol)	117
Add a Software Image from a Client Machine File System	117
Change the Device Requirements for Upgrading a Software Image	118
Verify That Devices Meet Image Requirements (Upgrade Analysis)	118
Distribute a New Software Image to Devices	119
Activate a New Software Image on Devices	126
Activate, Deactivate, and Remove Cisco IOS XR Images from Devices	128
View and Upgrade FPD Images	129
Commit Cisco IOS XR Images Across Device Reloads	130
Roll Back Cisco IOS XR Images	130
Check the Network Audit for Software Image Operations	131
Delete Software Image Files from the Image Repository	132

---

**CHAPTER 6**

<b>Perform Configuration Audits Using Compliance</b>	<b>133</b>
How To Perform a Compliance Audit	133
Enable and Disable Compliance Auditing	134
Create a New Compliance Policy	134
Create Compliance Policy Rules	135
Examples—Rule Conditions and Actions	135
Example Conditions and Actions: DNS Servers Configured on Device	136
Example: Block Options	136
Example Conditions and Actions: Community Strings	137
Example Conditions and Actions: IOS Software Version	138
Example Conditions and Actions: NTP Server Redundancy	138
Create a Compliance Profile That Contains Policies and Rules	139
Run a Compliance Audit	139
View the Results of a Compliance Audit	140
View Violation Job Details	141
View Change Audit Details	141

View Audit Failure and Violation Summary Details	142
Fix Device Compliance Violations	143
View Audit Failure and Violation Summary Details	143
Import and Export Compliance Policies	144
View the Contents of a Compliance Policy XML File	144
View PSIRT and EoX Information	145
View Device Security Vulnerabilities	145
View Device Hardware and Software End-of-Life Report	145
View Field Notices for Device	146

---

## PART III

---

### Visualize the Network 147

## CHAPTER 7

### Visualize the Network Topology 149

Network Topology Overview	149
View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map	151
Filter Data in the Detailed Tables	153
Search for a Device in the Map	153
Determine What is Displayed in the Topology Map	153
Choose Which Device Group(s) to Display in the Network Topology Map	154
View the Contents of a Sub-Group in the Topology Map	154
Manually Add Devices and Networks to the Topology Map	155
Manually Add Links to the Topology Map	156
Delete a Manually Added Link	156
Rename a Link	157
Change Which Link and Device Types are Shown in the Network Topology Map	157
Show/Hide Alarms and Labels in the Topology Map	158
Save Global Preferences for the Map Display	158
Load Global Preferences for the Map Display	159
Isolate Specific Sections of a Large Topology Map	159
Get More Information About Devices	160
Get More Information About Links	160
Get a Quick Look at a Specific Link: Link 360 View	160
Link Serviceability States	161

Compare Link Information and Status	162
View a Specific Link in the Topology Map	163
View a Device Group's Links in a Network Topology Map	163
View Link Tables	164
Troubleshoot Link Issues	165
Show Bandwidth Utilization for Links on the Map	166
Define Color Thresholds for Link Bandwidth Utilization	168
View Fault Information for Devices and Links	169
Change the Layout of a Network Topology Map	169
Add a Background Image to the Network Topology	171
Visualize and Trace Circuits/VCs	171
Display Routes of a Circuit	172
Trace and Visualize the Full Route of a Circuit	172
Show Clock Synchronization Networks on a Network Topology Map	172
Show Routing Networks on the Topology Map	173
Save the Topology Map as an Image File	174
View Your Network on a Geographical Map (Geo Map)	175
Geo Map Overview	175
Device Groups in the Geo Map	176
Geo Map Setup	177
Identify Which Devices are not Showing on the Geo Map (Unmapped Devices)	177
Place Unmapped Devices on the Geo Map	178
Change the Location of a Device on the Geo Map	178
Change the Location of a Device in a Cluster	179
Remove a Device from the Geo Map	179
Remove a Clustered Device from the Geo Map	179
Identify the Members of a Cluster	180
Search for a Specific Location in the Geo Map	180
View Link Layers in the Geo Map	181
View and Manage Optical Fiber Paths in the Geo Map	181
Manage Fiber Paths	182
Associate Links to Fibers	183
Visualize Circuits/VCs on the Geo Map	183
Import Location Data	184

Import Device Locations from a CSV File	184
Import Location Data from a KML File	185
Export Location Data from the Geo Map	187
View and Manage Shared Risk Resource Groups (SRRG) in the Geo Map	188
View Assigned and Unassigned SRRGs	188
Manage SRRG Assignments	189

---

## PART IV

---

### Monitor the Network 191

## CHAPTER 8

### Monitor Device and Network Health and Performance 193

How Device Health and Performance Is Monitored: Monitoring Policies	193
Set Up Basic Device Health Monitoring	194
Set Up Basic Interface Monitoring	195
Use the Dashboards To Check Network and Device Health	197
Check What Cisco EPN Manager Is Monitoring	198
Check Which Parameters and Counters Are Polled By a Monitoring Policy	200
Policies Pane Pop-Up Window	201
Check a Monitoring Policy's Device, Polling, Threshold, and Alarm Settings	201
Adjust What Is Being Monitored	201
Create a New Monitoring Policy Based On An Existing Policy	202
Create a New Monitoring Policy Using Out-of-the-Box Policy Types	203
Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices	203
Check the Status of Past Monitoring Policy Data Collections	204
Change the Device Set a Policy is Monitoring	204
Change the Polling for a Monitoring Policy	205
Change Thresholds and Alarm Behavior for a Monitoring Policy	205
Run Performance Tests	206
Run a Performance Test on a Link (OTS Link)	207
Configure OTDR Port Values	207
Provision OTDR Scan Recurrence	209
Run the OTDR Test	209
Export the OTDR Scan Result	210
View OTDR Scan Results in the Geo Map	211
Monitor Network Performance Using Reports	212

---

**CHAPTER 9****Monitor Alarms and Events 213**

- What Are Alarms and Events? 213
- How are Alarms and Events Created and Updated? 214
  - Example: Link Down Alarm 215
  - Flapping Events and Flow Controllers 216
- Which Events Are Supported? 217
- Set Alarm and Event Management Preferences 217
  - Set Up Your Alarm and Event Display Preferences 218
  - View Critical Alarm Notifications 219
  - Customize the Alarm Summary 220
- Interpret Event and Alarm Badges and Colors 221
  - Alarm Severity Icons 221
- Find and View Alarms 221
  - Device Timestamp and CEPNM Timestamp 223
- View a Specific Alarm in the Topology Map 223
- View Root Cause and Correlated Alarms 224
- Get Troubleshooting and Detailed Alarm Information 225
  - View an Alarm's Details 225
  - Find Troubleshooting Information for an Active Alarm 225
  - Find Out Which Events Are Associated With An Alarm 226
  - Find Out If An Alarm Impacts Other Services or Network Elements 226
- Acknowledge and Clear Alarms 227
  - Not Acknowledged 227
  - Acknowledged 227
  - Cleared 227
    - What are the Supported Alarm Clearing Mechanisms 228
- Add Notes To an Alarm 228
- Forward Alarms and Events as Email Notifications 229
- Manage How Alarms are Triggered (Alarm Thresholds) 229
- View Events (Including Generic Events) 230
- View Syslogs (Historic) 230
  - View Live Syslogs 231
- Export Alarms or Events to a CSV or PDF File 232



Get Support from Cisco	232
Respond to Problems Within Cisco EPN Manager	232

---

## CHAPTER 10

### Monitor Cisco ASR 9000 Network Virtualization (nV) Satellites and Cluster Services 233

Monitor Cisco ASR 9000 nV Satellites	233
Satellite Considerations in Cisco EPN Manager	234
Minimum Device and OS Requirements for Cisco ASR 9000 nV Satellites	235
Get Quick Information About a Specific Satellite: Satellite 360 View	235
View Cisco ASR 9000 Host-Satellite Topologies in the Topology Map	235
Identify the Satellites Connected to a Cisco ASR 9000 Host	236
Identify the Hosts Connected to a Satellite	238
Monitor Cisco ASR 9000 nV Satellites for Faults	238
View Satellite Faults in a Topology Map	239
View Satellite Faults Using a Device 360 View	239
View Satellite Faults in the Alarms and Events Table	240
Monitor a Cisco ASR 9000 nV Edge Cluster	241
Minimum Device and OS Requirements for nV Edge	241
View a nV Edge Cluster in the Topology Map	241
Identify the Primary and Backup Devices in a Cluster	242
Monitor and Troubleshoot a Cisco ASR 9000 nV Edge Cluster Service	243

---

## CHAPTER 11

### Manage Reports 245

Reports Overview	245
Available Reports	245
Carrier Ethernet Performance Reports	246
Optical Performance Reports	253
Performance Reports	258
Network Summary Reports	258
Device Reports	259
Create, Schedule, and Run a New Report	261
Customize Report Results	262
Report Output Examples: Web GUI Output and CSV File Output	262
Troubleshooting Tips for an Empty Report	264

---

**PART V**

---

**Configure Devices 265**

---

**CHAPTER 12****Configure Devices 267**

Ways to Configure Devices Using Cisco Evolved Programmable Network Manager 267

Which Devices Support the Configuration Operations? 268

Identify the Commands Used In a CLI Configuration Template 269

Save Your Device Changes 269

Save Device Configuration Changes to the Database (Update) 269

Collect a Device's Inventory Now (Sync) 269

Change a Device's Credentials and Protocol Settings 270

Change Basic Device Properties 271

Enable and Disable Interfaces 272

Configure Physical Attributes of Device Interfaces 272

Configure Circuit Emulation 275

Pre-requisites for Configuring CEM Services 276

Configure Interfaces for CEM 276

Configure APS and UPSR Protection Groups 279

Configure Clocking for CEM 281

CEM Interface (PDH, SONET, and SDH) Field Descriptions 282

Configure Alarm Profiles on Ports, Cards, and Nodes of Devices 285

Synchronize the Clock Using Sync-E, BITS, and PTP 288

Configure IP SLAs (TWAMP Responder) 293

Configure Interfaces 294

Configure Ethernet Interfaces and Subinterfaces 295

Configure Loopback Interfaces 296

Configure Tunnel Interfaces 297

Configure SwitchPort Interfaces 298

Configure Virtual Template Interfaces 298

Configure VLAN Interfaces 299

Configure Optical Interfaces 300

Change the Loopback Settings on an Optical Interface 300

Continuous Verification of the Connection Status 301

Configure PRBS on ODU Controllers 303

Enable and Disable OSC	304
View and Acknowledge Unverified Alarms	305
Provision Optical Interfaces	305
Example: Change the Admin Status for Cisco NCS 2006 Interface	318
Configure Devices Using the Chassis View	320
Create and Manage Users and User Logins for a Device	321
Configure Patchcords for a Device	322
Configure a Protection Group for a Shelf in a Device	323
Configure Slices	324
Configure Controllers (Optics, OTS, OCH, DSP, and DWDM)	325
Configure Passive Units	327
Edit Amplifier Module Settings on Optical Cards	328
Configure GMPLS and WSON Properties	329
Configure Optical Cards	331
Configure Cards from the Chassis View	331
Delete a Card	332
Reset a Card	332
Configure cards: OTU2-XP, MR-MXP, WSE, AR-XPE, AR-XP, AR-MXP, 40E-MXP-C, and 40ME-MXP-C	333
Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC	334
Configure SONET and Flex Line Cards	337
Edit and Delete Pluggable Port Modules and Card Mode Configuration	340
Cards and Supported Configuration for Cisco NCS 2000 Devices	341
Discover and Configure MPLS LDP and MPLS-TE Links	345
Analyze Ports Using SPAN and RSPAN	348
Configure and View Ethernet Link Aggregation Groups	350
Create Link Aggregation Groups (LAG) Using Multiple Interfaces	350
View Ethernet LAG Properties	351
Configure Routing Protocols and Security	352
Configure BGP	352
Configure EIGRP	355
Configure an IS-IS	356
Configure OSPF	358

Configure RIP	360
Configure Static Routing	361
Configure ACLs	361
Configure EOAM Fault and Performance Monitoring	362
Configure CFM	362
CFM Overview	363
Configure CFM Maintenance Domains and Maintenance Associations (Services)	364
Perform EOAM Connectivity and Performance Checks	366
Configure Quality of Service (QoS)	369
Create a QoS Classification Profile	370
Create a QoS Action Profile	372
Create a QoS Sub-Action Profile	376
Import and Export QoS Action and Sub-Action Profiles	377
Check Which QoS Profiles are Configured on a Device	377
Apply a QoS Action Profile to Interface(s)	378
Import QoS Profiles Discovered from Devices	378
Dissociate a QoS Action Profile from Multiple Interfaces	379
Delete QoS Classification and Action Profiles from Devices	380
Launch Cisco Transport Controller to Manage Cisco NCS and Cisco ONS Devices	381

---

**CHAPTER 13**

<b>Create Templates To Automate Device Configuration Changes</b>	<b>383</b>
Why Create New Configuration Templates?	383
Ways to Create Configuration Templates Using Cisco EPN Manager	384
Create a New CLI Configuration Template Using a Blank Template	384
Create a New CLI Configuration Template Using An Existing Template	385
Entering Variables in a Template	386
Data Types	386
Manage Database Variables in CLI Templates	387
Use Validation Expressions	387
Add Multi-line Commands	388
Add Enable Mode Commands	389
Add Interactive Commands	389
Use Global Variables in a Template	390
Import and Export a CLI Configuration Template	393

Create a New Composite Template	394
Create a Shortcut to Your Templates Using Tags	394
Deploy Templates to Devices	394
Create Configuration Groups for Deploying Templates to Groups of Devices	395
Deployment Flow for Configuration Templates Using the Wizard	395
Deployment Flow for CLI Templates using the Wizard	396
Deployment Flow for Composite Templates Using the Wizard	397
Deploy Templates to Devices Without Using Configuration Groups	398
Check the Status and Results of a Deployed Configuration Template	399

---

## CHAPTER 14

### Manage Cable Devices 401

Manage Cable Devices	401
Features and Limitations	402
Cable Management Features and Supported User Groups	402
Configure Client Credentials for Cable Devices	405
Add Cable Devices	406
Manage Cisco cBR-8 and RPDs Association	406
RPD Device Parameters and Descriptions	407
View and Export Cable Device Information and Configuration Details	408
Monitor the Health of RPD to cBR-8 Links	410
View the Cable Dashboard	411
Visualize the Topology of Cable Devices on the Network Topology	411

---

## PART VI

### Manage Circuits 413

---

## CHAPTER 15

### Overview of Circuit/VC Discovery and Provisioning 415

Circuits/VCs Provisioning Overview	415
Supported Carrier Ethernet VCs	416
Core Technology for Multipoint EVCs	416
E-Line	417
E-LAN	417
E-Tree	418
E-Access	418
EVPN Virtual Private Wire Service (VPWS)	419

Supported Network Structure for Provisioning EVCs	419
Supported Optical Circuits	419
Dense Wavelength Division Multiplexing (DWDM) Circuits	420
Optical Channel Network Connection (OCHNC) WSON	420
Optical Channel Client Connection (OCHCC) WSON	420
Optical Channel (OCH) Trail WSON	421
Optical Channel (OCH) Trail Connecting NCS 1002, NCS 55xx, and ASR 9K Devices	421
Optical Channel (OCH) Trail Hybrid Circuits	421
Optical Channel (OCH) Trail User-to-Network Interface (UNI)	422
Spectrum Switched Optical Network (SSON) Circuits	422
Optical Transport Network (OTN) Circuit	423
Optical Channel Data Unit User-to-Network Interface (ODU UNI)	424
Optical Channel Data Unit (ODU) Tunnel	424
Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU)	425
Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin	425
Optical Channel Data Unit (ODU)	425
Supported Circuit Emulation Services	425
Supported L3VPN Services	427
Supported MPLS Traffic Engineering Services	428
Unidirectional TE Tunnel	428
Bidirectional TE Tunnel	429
Layer 3 Link	429
Supported Serial Services	429
Circuit/VC Discovery Overview	430

---

**CHAPTER 16**
**Provision Circuits/VCs 431**

Provision Circuits/VCs in Cisco EPN Manager	431
Set the Service Deployment Timeout Value	433
What Happens When a Deployment Fails	433
Troubleshoot Configuration Deployment Failures and Roll Back Failures	435
Provision EVCs in a Carrier Ethernet Network	436
Summary of Cisco EPN Manager Carrier Ethernet Provisioning Support	436
Prerequisites for EVC Provisioning	436
Create and Provision a New Carrier Ethernet EVC	437

Create and Provision an EVC with Multiple UNIs	439
Service Details Reference	441
New UNI Details Reference	442
UNI Service Details Reference	443
Service OAM	444
Configure a Device and Interface To Be a UNI	445
Configure a Device and Interface To Be an ENNI	446
Provision Circuits in an Optical/DWDM Network	447
Summary of Cisco EPN Manager Optical/DWDM Network Provisioning Support	447
Prerequisites for Provisioning Optical Circuits	448
Create and Provision an OCH Circuit	449
Circuit Section Reference for OCH Circuit Types	450
Create and Provision Two Mutually Diverse OCH-Trail UNI Circuits	454
Create and Provision a Media Channel Group SSON Circuit	456
Create and Provision a Media Channel SSON Circuit	457
Circuit Section Reference for Media Channel SSON Circuit Types	458
Create and Provision an OTN Circuit	460
Circuit Section Reference for OTN Circuit Types	461
Endpoint Section Reference for OTN Circuit Types	463
Bandwidth and Service Type Value Mapping for ODU UNI Circuits.	465
Create and Provision an ODU Circuit	466
Provision L3VPN Services	467
Supported L3VPN Services	467
L3VPN Provisioning Features and Limitations	468
Prerequisites for L3VPN Provisioning	469
L3VPN Service Discovery	470
Create and Provision a New L3VPN Service	471
PE-CE Routing Details References	478
Example Configuration: Provisioning an L3VPN Service	479
View L3VPN Service Details	481
Modify L3VPNs and VRFs	481
Add and Copy VRFs to an L3VPN Service	482
Provision Circuit Emulation Services	483
Summary of Cisco EPN Manager CEM Provisioning Support	483

Prerequisites for CEM Provisioning	483
Create and Provision a New CEM Service	483
CEM Service Details References	485
Provision MPLS Traffic Engineering Services	489
Summary of Cisco EPN Manager MPLS TE Provisioning Support	489
MPLS TE Service Provisioning Features	489
Prerequisites for Provisioning an MPLS TE Service	490
Create and Provision an MPLS TE Tunnel	490
Field References for Service Details—MPLS TE Tunnel	491
Field References for Tunnel Creation—MPLS TE Tunnel	492
Field References for Path Constraint Details—MPLS TE Tunnel	496
Create and Provision an MPLS Layer 3 Link	498
Field References for A End Details and Z End Details in MPLS Layer 3 Link	499
Provision Serial Services	503
Prerequisites for Serial Circuits/VCs Provisioning	503
Create and Provision a New Serial Circuit/VC	504
Serial Service Details Reference	505
Create and Provision a New Raw Socket Circuit/VC	507
Raw Socket Service Details Reference	508
Create Circuit/VC Profiles	509
Create QoS Profiles	510
Create Customers	511
Provision a Circuit/VC with an Unmanaged Endpoint	511
Extend a Circuit/VC Using Templates	512
Example Configuration: Extend a Circuit/VC Using CLI Templates	513
 <b>CHAPTER 17</b>	
<b>View and Manage Discovered/Provisioned Circuits/VCs</b>	<b>519</b>
Enable and Disable Service Discovery	519
Circuit or VC States	520
View Circuits/VCs	525
View a Specific Circuit/VC's Details	525
View a Specific Circuit/VC in the Topology Map	525
Get Quick Information About a Circuit/VC: Circuit/VC 360 View	528
Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window	532



View and Compare Versions of a Circuit (Optical)	533
View a Specific Device's Circuits/VCs	534
View a Device Group's Circuits/VCs	535
View a Device Group's Circuits/VCs List in the Topology Window	535
View a Device Group's Circuits/VCs in an Expanded Table	535
View All Circuits/VCs in Cisco EPN Manager	536
Identify and Manage Discovered Circuits/VCs	537
Show/Hide Implicit Circuits	537
Filter and Export the Circuit/VC list Based on a User Defined Field	538
Display the Routes Associated With a Circuit	539
Promote a Discovered Circuit/VC Before Modifying/Deleting	539
Modify a Circuit/VC	540
Activate a Circuit (Optical)	541
Restore a Circuit (Optical)	541
Reroute a Circuit (Optical)	542
Compare and Reconcile Provisioned and Discovered Versions of a Circuit/VC	543
Initiate a Protection Switch Action on a Circuit (Optical)	544
Delete a Circuit/VC	546
Delete an L3VPN Service	547
Delete an L3VPN Service Endpoint	548
Delete an MPLS TE Service	548
Manage Provisioned Network Interfaces	549
Delete Network Interfaces	550

---

**CHAPTER 18**
**Monitor and Troubleshoot Circuits/VCs 551**

Check Circuits/VCs for Faults	551
Identify Which Circuits/VCs are Affected by a Specific Fault	552
Get More Information About a Circuit/VC Failure	553
Troubleshoot a Service Failure Using OAM Commands	554
Launching from Network Devices Table	555
Launching from Circuit 360	555
Launching from Alarm Browser	556
Perform a Ping or Traceroute Using OAM Command	557
Use EOAM Templates to Troubleshoot EVCs	558

Run a Performance Test on a Circuit/VC	558
Performance Test Based on Y.1564 for EVCs	558
Supported Devices	559
Running a Y.1564 Performance Test	560
Performance Test Based on Y1731 for EVCs	561
Performance Test for Optical Circuits	562
Optical Performance Monitoring Parameters	563
Run PRBS Test on Circuits (ODU UNI)	563
Performance Test for Circuit Emulation Services	565
View and Export the Results of the Performance Test on Circuit Emulation Services	566
View Performance Metrics and Reports for Circuits/VCs	566
View Performance Graphs in the Circuit/VC 360 View	567
Use Performance Reports to Monitor and Troubleshoot Circuits/VCs	567
Use Service Performance Dashboard to Monitor Circuits/VCs	567
Trace and Visualize the Full Route of Circuits/VCs	568
Three-Dimensional View of a Circuit V/C Trace	570
Linear View of a Circuit/VC Trace	571
View Specific Information of a Circuit in a Multilayer Trace View	572
Actions You Can Perform from the Multilayer Trace View	574

---

**PART VII**
**Administer the Cisco EPN Manager System 577**


---

**CHAPTER 19**
**Set Up the Cisco EPN Manager Server 579**

Server Setup Tasks	579
User Management Setup Tasks	581
Fault Management Setup Tasks	581
Web GUI Setup Tasks (Admin)	582
Customize the Web GUI Menus to Disable Cisco EPN Manager Features	582

---

**CHAPTER 20**
**Licenses and Software Updates 585**

View and Manage Licenses	585
Types of Cisco EPN Manager Licenses	585
Base License	585
Device Right-to-Manage (RTM) License	586

SBY License for High Availability	586
NBI License	586
Time-Based, Lab, and Permanent Licenses	586
Use Cisco Smart Licensing	586
Set Up Cisco Smart Licensing in Cisco EPN Manager	587
Choose Cisco EPN Manager Licenses Using Smart Licensing	590
Convert Traditional Licenses to Smart Entitlements	590
Configure License Thresholds for the Smart License Dashboard	591
Check Cisco EPN Manager License Usage	591
Disable Smart Licensing	591
Reference: Smart Product Registration and License Authorization Statuses	592
Use Traditional Licensing	593
View Traditional Licenses	593
Add and Delete Traditional Licenses	593
Move a Traditional License to Another Server	594
Renewing an Expired License	594
View the Licensing Dashboard	595
Manage Software Updates	596
What Are Software Updates?	596
View the Installed Product Software Version	596
View Installed Software Updates	597
Enable or Disable Notifications About Software Updates	597
 <b>CHAPTER 21</b>	
<b>Cisco EPN Manager Security</b>	<b>599</b>
Security Overview	599
Secure Architecture	599
Ports Used by Cisco EPN Manager	601
Secure Default Configurations	603
Harden Your Installation	603
Configure the Built-In Application Firewall	604
Set Up Exterior Network Firewalls	605
Set Up Traffic Encryption	606
Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices	607
Set Up External Authentication Using the CLI	607

Harden SSH Against Brute-Force Password Attacks	608
Harden NTP	610
Set Up NTP on the Cisco EPN Manager Server	610
Enable Authenticated NTP Updates	610
Configure External NFS-Based Storage Servers	611
CSDL Process	611
Cisco Security Issue Resolution Process	612

---

**CHAPTER 22**
**Backup and Restore 613**

Backup and Restore Concepts	613
Backup Types: Application and Appliance	613
Backup Scheduling	614
Backup Repositories	614
Backup Filenames	615
Backup Validation Process	615
Information That Is Backed Up	616
Information That Is Not Backed Up	618
Set Up and Manage Repositories	618
Create a Local Backup Repository	618
Use a Remote Backup Repository	619
Use Remote NFS Backup Repositories	619
Use Remote FTP Backup Repositories	621
Use Remote SFTP Backup Repositories	622
Delete a Local Backup Repository	623
Set Up Automatic Application Backups	623
Schedule Automatic Application Backups	624
Specify the Backup Repository for Automatic Backups	624
Change the Number of Automatic Application Backups That Are Saved	625
Perform a Manual Backup	625
Perform an Immediate Application Backup	625
Perform an Immediate Application Backup Using the Web GUI	625
Perform an Immediate Application Backup Using the CLI	626
Perform a Manual Appliance Backup	626
Restore Cisco EPN Manager Data	626

Restore an Application Backup	627
Restore an Appliance Backup	627
Recover from Failed Restores	628
Manage Disk Space Issues During Backup and Restore	629
Migrate to Another Virtual Appliance Using Backup and Restore	629

---

## CHAPTER 23

### Server Health and Configuration 631

View the Cisco EPN Manager Server Configuration	631
Change the Cisco EPN Manager Hostname	632
Connect via CLI	632
Secure the Connectivity of the Cisco EPN Manager Server	633
Set Up HTTPS to Secure the Connectivity of the Web Server	633
Generate and Apply Self-Signed Web Server Certificate	634
Generate and Apply a CA-Signed Web Server Certificate	635
Change the HTTPS Server Port	643
View Existing CA Certificates	643
Delete CA Certificates	643
Establish an SSH Session With the Cisco EPN Manager Server	644
Set Up NTP on the Server	644
Set Up the Cisco EPN Manager Proxy Server	645
Set Up the SMTP E-Mail Server	645
Enable FTP/TFTP/SFTP Service on the Server	646
Configure Stored Cisco.com Credentials	646
Create a Login Banner (Login Disclaimer)	647
Stop and Restart Cisco EPN Manager	647
Configure Global SNMP Settings for Communication with Network Elements	647
Manage Administrative Passwords	648
Change the FTP User Password	648
Change the Web GUI Root User Password	649
Recovering Administrator Passwords on Virtual Appliances	649
Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard	650
Improve the Cisco EPN Manager Server Performance	651
Check the OVA Size	651

Compact the Database	651
Manage Server Disk Space Issues	651
Work With Server Internal SNMP Traps That Indicate System Problems	652
Customize Server Internal SNMP Traps and Forward the Traps	652
Troubleshoot Server Internal SNMP Traps	653
Set Up Defaults for Cisco Support Requests	654
Configure Cisco Product Feedback Settings	654

---

**CHAPTER 24**
**Data Collection and Purging 655**

Control Data Collection Jobs	655
About System Jobs	655
How Data Retention Settings Affect Web GUI Data	663
Performance and System Health Data Retention	663
Alarm, Event, and Syslog Purging	664
Log Purging	665
Report Purging	665
Backup Purging	665
Device Configuration File Purging	666
Software Image File Purging	666

---

**CHAPTER 25**
**User Permissions and Device Access 667**

User Interfaces, User Types, and How To Transition Between Them	667
User Interfaces and User Types	667
How to Transition Between the CLI User Interfaces in Cisco EPN Manager	669
Transition Between the Cisco EPN Manager admin CLI and Cisco EPN Manager config CLI	669
Log In and Out as the Linux CLI root User	670
Enable and Disable root Access for the Linux CLI and the Cisco EPN Manager Web GUI	671
Disable and Enable the Linux CLI Users in Cisco EPN Manager 2.x	671
Disable and Enable the Web GUI root User	671
Control the Tasks Users Can Perform (User Groups)	672
Types of User Groups	672
User Groups—Web UI	672
User Groups—NBI	673

View and Change the Tasks a User Can Perform	674
View and Change the Groups a User Belongs To	674
View User Groups and Their Members	675
Create a Customized User Group	675
View and Change the Tasks a Group Can Perform	676
Use Cisco EPN Manager User Groups with RADIUS and TACACS+	676
Export the Cisco EPN Manager User Group and Task List Attributes for RADIUS and TACACS+	676
Add Users and Manage User Accounts	677
Create Web GUI Users with Administrator Privileges	678
Add and Delete Users	678
Disable (Lock) a User Account	679
Change a User's Password	679
Find Out Which Users Are Currently Logged In	679
View the Tasks Performed By Users (Audit Trail)	680
Configure Job Approvers and Approve Jobs	680
Configure Global Password Policies for Local Authentication	681
Configure the Global Timeout for Idle Users	681
Disable Idle User Timeout	682
Create Virtual Domains to Control User Access to Devices	682
What Are Virtual Domains?	682
How Virtual Domains Affect Cisco EPN Manager Features	683
Reports and Virtual Domains	683
Search and Virtual Domains	683
Alarms and Virtual Domains	684
Maps and Virtual Domains	684
Configuration Templates and Virtual Domains	684
Config Groups and Virtual Domains	684
Email Notifications and Virtual Domains	684
Create New Virtual Domains	684
Create Virtual Domains Directly Under ROOT-DOMAIN	685
Create Child Virtual Domains (Subdomains)	685
Import a List of Virtual Domains	687
Add Network Devices to Virtual Domains	687

Assign Virtual Domains to Users	687
Edit a Virtual Domain	688
Delete a Virtual Domain	688
Use Cisco EPN Manager Virtual Domains with RADIUS and TACACS+	689
Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+	689
Configure Local Authentication	690
Use SSO With Local Authentication	690
Configure External Authentication	691
Use RADIUS or TACACS+ for External Authentication	691
Add a RADIUS or TACACS+ Server to Cisco EPN Manager	691
Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server	692
Use Cisco ISE With RADIUS or TACACS+ for External Authentication	692
Supported Versions of Cisco ISE in Cisco EPN Manager	693
Add Cisco EPN Manager as a Client in Cisco ISE	693
Create a User Group in Cisco ISE	694
Create a User and Add the User to a User Group in Cisco ISE	694
Create an Authorization Profile for RADIUS in Cisco ISE	694
Create an Authorization Profile for TACACS+ in Cisco ISE	695
Configure an Authorization Policy in Cisco ISE	696
Create an Authentication Policy in Cisco ISE	697
Use Cisco ACS With RADIUS or TACACS+ for External Authentication	697
Supported Versions of Cisco ACS in Cisco EPN Manager	698
Add Cisco EPN Manager as a Client in Cisco ACS	698
Create a User Group in Cisco ACS	699
Create a User and Add the User to a User Group in Cisco ACS	699
Create an Authorization Profile for RADIUS in Cisco ACS	699
Create an Authorization Profile for TACACS+ in Cisco ACS	700
Create an Access Service for Cisco EPN Manager in Cisco ACS	701
Create an Authorization Policy Rule in Cisco ACS	702
Configure a Service Selection Policy in Cisco ACS	702
Use SSO with External Authentication	703
Add the SSO Server	703
Configure SSO Mode on the Cisco EPN Manager Server	703



**CHAPTER 26****Fault Management Administration Tasks 705**

- Event Receiving, Forwarding, and Notifications 705
  - Forward Alarms and Events as Email Notifications (Administrator Procedure) 706
    - Configure Default Settings for E-Mail Notifications 707
  - Forward Alarms and Events as SNMP Trap Notifications 707
- Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms 708
- Change Event Severity Levels 709
- Customize the Troubleshooting Text for an Alarm 710
- Change Alarm Auto-Clear Intervals 710
- Change the Information Displayed in the Failure Source for Alarms 711
- Change the Behavior of Expedited Events 711
- Customize Generic Events That Are Displayed in the Web GUI 712
  - Disable and Enable Generic Trap and Syslog Handling 712
    - Disable and Enable Generic Trap Processing 712
    - Disable and Enable Generic Syslog Processing 712
  - Customize Generic Events Based on SNMP Traps 713
- Troubleshoot Fault Processing Errors 713
- Get Help from the Cisco Support Community and Technical Assistance Center (TAC) 714
  - Open a Cisco Support Case 714
  - Join the Cisco Support Community 715

**CHAPTER 27****Audits and Logs 717**

- Audit Configuration Archive and Software Management Changes (Network Audit) 717
- Audit Changes Made By Users (Change Audit) 717
  - Generate a Change Audit Report 717
  - Enable Change Audit Notifications and Configure Syslog Receivers 718
- Audit Actions Executed from the GUI (System Audit) 719
- System Logs 719
  - View and Manage General System Logs 720
    - View the Logs for a Specific Job 720
    - Adjust General Log File Settings and Default Sizes 720
    - Download and E-Mail Log Files for Troubleshooting Purposes 721
    - Forward System Audit Logs As Syslogs 721

Enable SNMP Traces and Adjust SNMP Log Settings (Levels, Size) 721

## CHAPTER 28

### Configure High Availability 723

How High Availability Works 723

HA States and Transitions 725

Set Up High Availability 727

Using Virtual IP Addressing With HA 728

What If I Cannot Use Virtual IP Addressing? 728

Register the Secondary Server for HA 729

What Happens During Secondary Server Registration 729

Register the Secondary Server on the Primary Server 729

Troubleshoot an HA Registration Failure 730

Configure an SSO Server in an HA Environment 731

Reset the HA Authentication Key 731

Reset the Server IP Address or Host Name 732

Restore Data In an HA Deployment 732

Monitor HA Status and Events 732

Use the Health Monitor Web Page 732

HA Configuration Modes 734

Check HA Status and Overall Health 734

View and Customize HA Events 735

Use HA Error Logging 735

Trigger Failover 736

Trigger Failback 736

Common Failover/Failback Scenarios 737

Network is Down 738

Process Restart Fails 738

Primary Server Restarts During Synchronization 739

Secondary Server Restarts During Synchronization 739

How to Recover From Split-Brain Scenario 739

Both HA Servers Are Powered Down 739

Both HA Servers Are Down and Secondary Server Will Not Restart 740

Replace the Primary HA Server 741

Secondary Server Goes Down 741

High Availability CLI Command Reference 742

---

## APPENDIX A

### Best Practices: Harden Your Cisco EPN Manager Security 743

Core Security Concepts 743

HTTPS 743

SSL Certificates 744

1-Way SSL Authentication 744

Cisco EPN Manager Security Hardening Overview 745

Harden the Cisco EPN Manager Web Server 746

Make Web Server Connectivity Secure By Using HTTPS 746

Set Up Certificate-Based Authentication for Web Clients 746

Configure and Manage OCSP on the Server 749

Configure a Custom OCSP Responder on the Server 749

Delete a Custom OCSP Responder from the Server 749

Harden the Cisco EPN Manager Server 749

Disable Insecure Ports and Services 750

Disable Accounts Not Needed for Day-to-Day Operations 751

Harden Your Cisco EPN Manager Storage 751

Harden NFS-Based Storage 751

---

## APPENDIX B

### Icon and State Reference 753

Device Reachability and Admin States 753

Port or Interface States 755

Circuit or VC States 756

Link Serviceability States 761

Link Characteristics 761

Equipment Operational States (Chassis View) 762

Alarm Severity Icons 762

Device Type Icons 763

Circuit or VC Network Topology Overlay Icons 765

---

## APPENDIX C

### Monitoring Policies Reference 767

Device Health Monitoring Policy 767

Interface Health Monitoring Policy 768

Custom MIB Polling Monitoring Policy	768
IP SLA Y.1731 Monitoring Policy	768
Pseudowire Emulation Edge to Edge Monitoring Policy	769
Quality of Service Monitoring Policy	769
IP SLA Monitoring Policy	770
ME1200 EVC QoS Monitoring Policy	770
BNG Sessions and IP Pools Monitoring Policy	771
TDM/SONET Ports Monitoring Policy	771
Optical SFP Monitoring Policy	771
Optical 1 Day and Optical 15 Mins Monitoring Policies	772
CEM Monitoring Policy	772
Device Sensor Monitoring Policy	773
Performance Counters for Optical Monitoring Policies	773
Reference—Performance Counters for Physical Interfaces	773
Reference—Performance Counters for OTN-FEC Interfaces	775
Reference—Performance Counters for OTN-ODU Interfaces	775
Reference—Performance Counters for OTN-OTU Interfaces	776
Reference—Performance Counters for Ethernet Interfaces	777
Reference—Performance Counters for SONET Interfaces	779
Reference—Performance Counters for SDH Interfaces	779



## PART I

# Get Started with Cisco EPN Manager

- [Get Started With Cisco EPN Manager](#) , on page 1





# CHAPTER 1

## Get Started With Cisco EPN Manager



**Note** If you are an administrator and need to set up Cisco EPN Manager for its initial use, see [Server Setup Tasks](#), on page 579.

- [Web Client Requirements](#), on page 1
- [Log In and Out](#), on page 2
- [Setup Tasks That Should Be Completed Before Using Cisco EPN Manager](#), on page 2
- [Change Your Password](#), on page 3
- [Use the Main Window Controls](#), on page 3
- [Change Your Default Home Page](#), on page 5
- [Set Up and Use the Dashboards](#), on page 6
- [Work In a Different Virtual Domain](#), on page 24
- [Manage Jobs Using the Jobs Dashboard](#), on page 25
- [Extend Cisco EPN Manager Functions](#), on page 26
- [Check Cisco.com for the Latest Cisco EPN Manager Documentation](#), on page 27

## Web Client Requirements

The following are the client and browser requirements for the Cisco EPN Manager Web GUI:

- Hardware—Mac or Windows laptop or desktop compatible with one of the tested and supported browsers listed below.
- Browsers:
  - Google Chrome versions 44 to 64
  - Mozilla Firefox ESR 38
  - Mozilla Firefox versions 39 to 58.0.1
  - Microsoft Internet Explorer (IE) 11.0



**Note** Internet Explorer users have reported slower performance compared to other browsers, meaning that some GUI pages take longer to load in IE.

- Recommended display resolution—1600x900 pixels or higher (minimum: 1366x768)

**Note**

A maximum of three Cisco EPN Manager tabs can be open simultaneously in a single browser session.

## Log In and Out

To log into the GUI, enter the following in your web browser address field, where *server-ip* is the IP address of the Cisco EPN Manager server:

**https://server-ip**

Depending on your network configuration, the first time your browser connects to the Cisco EPN Manager web server, you may have to update your client browser to trust the server's security certificate. This ensures the security of the connection between your client and the Cisco EPN Manager web server.

To log out, click  at the top right of the Cisco EPN Manager window and choose **Log Out**.

For information on Cisco EPN Manager users and the actions they can perform, see:

- [How to Transition Between the CLI User Interfaces in Cisco EPN Manager](#), on page 669—Describes all classes of users supported by Cisco EPN Manager, including the various CLI user accounts.
- [Types of User Groups](#), on page 672—Describes the user group mechanism which allows you to control the functions that everyday web GUI users can perform. What you can see and do in the user interface is controlled by your user account privileges. This topic also describes the virtual domain mechanism, which manages Role-Based Access Control (RBAC) for devices.

## Setup Tasks That Should Be Completed Before Using Cisco EPN Manager


Before you can use the Cisco EPN Manager features, these tasks should be completed by an administrator:

**Table 1: Setup Tasks and References**

Tasks to completed before using Cisco EPN Manager	For information, see:
Set up and configure the Cisco EPN Manager server.	<a href="#">Server Setup Tasks</a> , on page 579
Add devices to Cisco EPN Manager and create device groups to simplify device and network management.	<a href="#">Add and Organize Devices</a> , on page 31
Enable monitoring for interfaces and technologies used by the network.	<a href="#">Monitor Device and Network Health and Performance</a> , on page 193
Customize alarm and event behavior for your deployment (for example, alarm and event refresh rates and e-mail and trap receivers).	<a href="#">Set Alarm and Event Management Preferences</a> , on page 217





# Change Your Password

You can change your password at any time by clicking  at the top right of the Cisco EPN Manager window and choosing **Change Password**. Click the information icon to review the password policy.


## Use the Main Window Controls


The top left of the Cisco EPN Manager title bar provides the following controls.


	Menu button—Toggles the main Cisco EPN Manager navigation menu on the left (also called the left sidebar menu)
	Home button—Returns you to the home page (normally the Overview Dashboard)

The right side of the title bar displays your user name and the virtual domain you are working in. A *virtual domain* is a logical grouping of devices. Virtual domains are used to control who has access to devices and areas of the network. To switch between virtual domains that are assigned to you, see [Work In a Different Virtual Domain](#), on page 24.



	Web GUI global settings button—Log out, change password, view your Cisco.com account profile, adjust your GUI preferences, check a Cisco.com support case, launch online help
-------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

When you click  on the right side of the title bar, the window settings menu opens.

jsmith - ROOT-DOMAIN 

**Logged In As jsmith**  
Log out  
Change Password  
Set Current Page As Home  
My Preferences  
Support Cases

Virtual Domain:ROOT-DOMAIN

**Help**  
Getting Started  
Online Help  
API Help  
Supported Devices

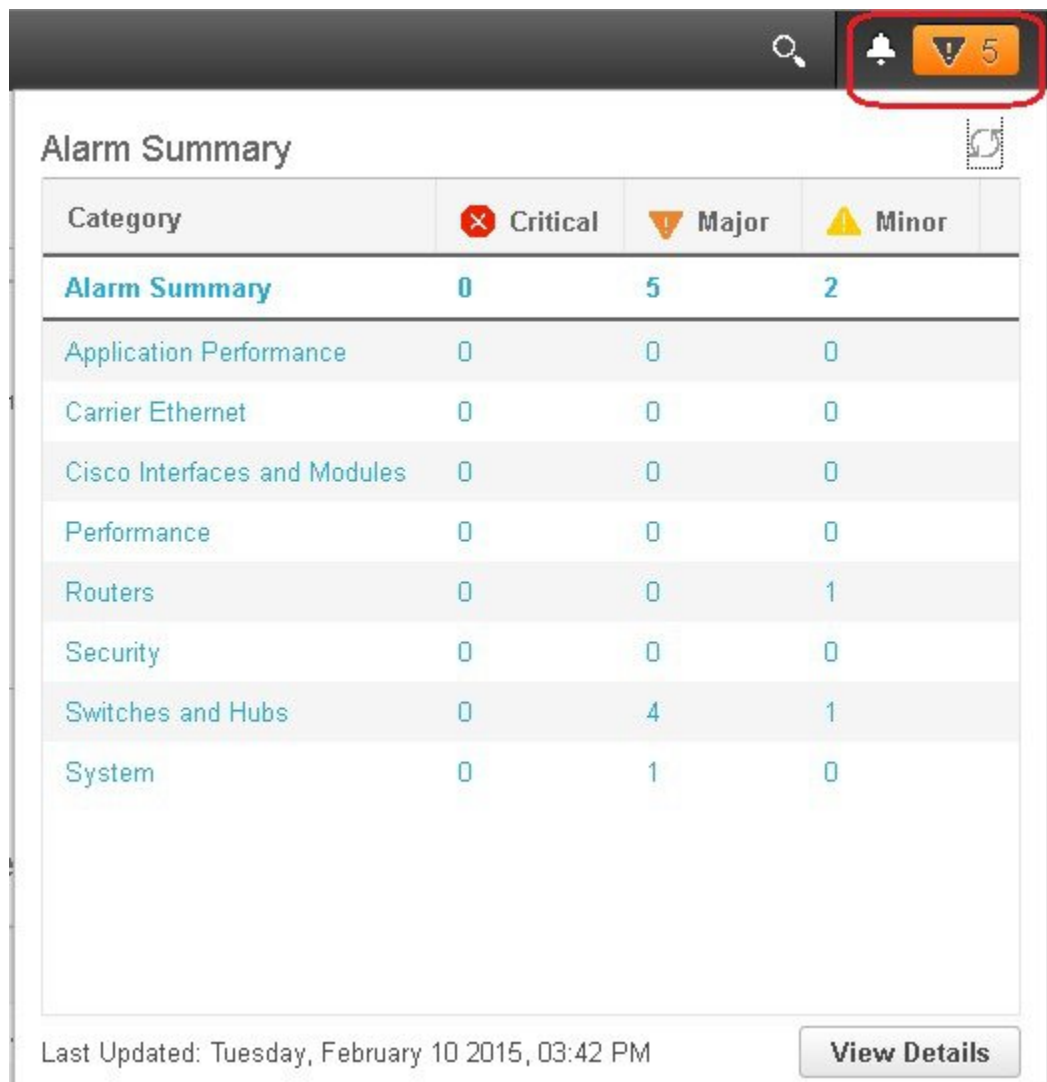
**Feedback**  
I wish this page would...  
About Cisco EPN Manager




414924

Finally, the Alarm Summary gives you a visual indicator of number of alarms in your network. The color indicates the highest severity alarm.

	Alarm Summary—Provides a visual count of alarms in the categories you specify. Clicking this area opens the <b>Alarm Summary</b> popup window.
-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------

When you click the **Alarm Summary** button (circled in the following figure), Cisco EPN Manager opens the **Alarm Summary** popup window. You can customize the data that is displayed in both the button and the pop-up window. In this example, the button displays a count for Switches and Hubs and System alarms, and the Alarm Summary pop-up to show all of the alarm categories listed in the following illustration.




Category	 Critical	 Major	 Minor
<b>Alarm Summary</b>	<b>0</b>	<b>5</b>	<b>2</b>
Application Performance	0	0	0
Carrier Ethernet	0	0	0
Cisco Interfaces and Modules	0	0	0
Performance	0	0	0
Routers	0	0	1
Security	0	0	0
Switches and Hubs	0	4	1
System	0	1	0


Last Updated: Tuesday, February 10 2015, 03:42 PM [View Details](#)

## Change Your Default Home Page

You can specify which page you want to display when you perform either of the following tasks:

- You click  from the left side of the web GUI title bar.
- You log in to the Cisco EPN Manager web GUI.

This setting is saved on a per-user basis. You can change it at any time without affecting other users.

- 
- Step 1** While you have the page you want displayed, click  at the top right of the Cisco EPN Manager web GUI.
- Step 2** Choose **Set Current Page as Home**.
-

# Set Up and Use the Dashboards

Dashboards provide at-a-glance views of the most important data in your network. They provide status as well as alerts, monitoring, performance, and reporting information. You can customize these dashboards so they contain only the information that is important to you. It may be helpful to set the **Network Summary** dashboard as your default home page. By doing so, this dashboard is displayed after you log in and you can quickly check overall network health before you do anything else. To set any dashboard as your default home page, see [Change Your Default Home Page, on page 5](#).

Use the following dashboards to monitor and manage your network:

- **Network Summary** dashboard—To check the health of the entire network. See [Network Summary Dashboard Overview](#).
- **Service Performance** dashboard—To monitor Carrier Ethernet and optical service performance. See [Service Performance Dashboard Overview](#).
- **Performance** dashboard—To view high-level performance metrics for network components such as interfaces, QoS policies, and ITU-T Y.1731 probes. See [Performance Dashboard Overview](#).
- **Device Trends** dashboard—To view performance information for a specific device, application, or service. See [Device Trends Dashboard Overview](#).
- **DWDM/OTN Performance** dashboard—To view performance information for the dense wavelength division multiplexing (DWDM) and Optical Transport Network (OTN) interfaces in your network. See [DWDM/OTN Performance Dashboard Overview](#).
- **Cable** dashboard —To view performance information for your cable network including the important issues currently affecting your network of Cisco cBR-8 devices. See [Cable Dashboard Overview, on page 15](#).

Users with administrator privileges can also use the following dashboards:

- **Licensing** dashboard—See [View the Licensing Dashboard](#)
- **Jobs** dashboard—See [Manage Jobs Using the Jobs Dashboard, on page 25](#).
- **System Monitoring** dashboard—See [Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard, on page 650](#).

Note the following:

- For an explanation of the parts of the dashboard window and how to use dashboard filters, see [How to Use the Dashboards, on page 18](#).
- To troubleshoot dashboard data issues, see [Find Out Why Data Is Missing from a Dashboard](#).

## Types of Dashboards

The following topics describe the dashboards available in Cisco EPN Manager.

## Service Performance Dashboard Overview

From the **Service Performance** dashboard, you can view the performance statistics for a particular circuit, VC, or service during the time frame you specify. To open this dashboard, choose **Dashboard > Service Performance** > any of the tabs described in the following table.

Dashboard Tab	Information Provided
CEM	<p>For the selected Circuit Emulation (CEM) circuit:</p> <ul style="list-style-type: none"> <li>• Details such as its name, type, and creation date</li> <li>• Statistics (you can toggle between the statistics for the circuit's endpoints)</li> <li>• Number of packets lost during transmission</li> <li>• Number of packets re-ordered in the jitter buffer before they reached their destination</li> <li>• Number of jitter buffer overruns and underruns</li> <li>• Number of packets ordered incorrectly and subsequently dropped</li> <li>• Number of malformed packets</li> <li>• Number of seconds that were errored, severely errored, or unavailable</li> <li>• Failed events</li> <li>• Dashlets that chart the number of Explicit Pointer Adjustment Relay counters (such L-bits and P-bits) that have been generated and received</li> </ul> <p><b>Note</b> To view these dashlets, both the CEM and Pseudowire Emulation Edge to Edge monitoring policies must be enabled. See <a href="#">Monitoring Policies Reference, on page 767</a>.</p>
TE Tunnel	<p>For the selected Traffic Engineering (TE) tunnel circuit:</p> <ul style="list-style-type: none"> <li>• Details such as its name, serviceability state, and associated endpoint</li> <li>• Service statistics</li> <li>• Outgoing traffic, bandwidth utilization, and reserved bandwidth</li> <li>• Service availability</li> </ul>

Dashboard Tab	Information Provided
CE/L3VPN	<p>For the selected circuit or VC:</p> <ul style="list-style-type: none"> <li>• Details such as its name, discovery state, and the last time it was modified</li> <li>• Lists the circuits and VCs with the highest values for the following parameters: <ul style="list-style-type: none"> <li>• Average traffic between endpoints</li> <li>• QoS class traffic and drops</li> </ul> </li> </ul> <p><b>Note</b> You can toggle between inbound and outbound data. In the <b>Top N Service QoS Class Traffic</b> dashlet, you can also toggle between pre- and post-policy data.</p> <ul style="list-style-type: none"> <li>• Inbound and outbound QoS drops</li> <li>• Service traffic and availability</li> <li>• Two-way delay, one-way jitter , and service loss</li> </ul>
Top CE/L3VPN	<p>Lists the circuits and VCs with the highest values for the following parameters:</p> <ul style="list-style-type: none"> <li>• Delay</li> <li>• Jitter</li> <li>• Service loss</li> <li>• Traffic (both inbound and outbound)</li> </ul> <p>You can toggle between the information for CE and L3VPN services.</p>

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

## Performance Dashboard Overview

From the **Performance** dashboard, you can view high-level performance metrics for network components such as interfaces, QoS policies, and ITU-T Y.1731 probes. To open this dashboard, choose **Dashboard > Performance >** any of the tabs described in the following table.

Dashboard Tab	Information Provided
Interfaces	<p>For the selected interface:</p> <ul style="list-style-type: none"> <li>• Details such as its name, the IP address of the device it is located on, and its configured speed</li> <li>• The average, minimum, and maximum values for the following performance metrics (you can toggle between the metrics collected for inbound and outbound data): <ul style="list-style-type: none"> <li>• Traffic</li> <li>• Utilization</li> <li>• Errors</li> <li>• Discards</li> <li>• Cyclic redundancy check (CRC) errors</li> </ul> </li> </ul> <p><b>Note</b> CRC error data is not polled by default. To enable the collection of this data, choose a polling frequency for the Interface Health monitoring policy's CRC parameter (see <a href="#">Change the Polling for a Monitoring Policy</a>).</p> <ul style="list-style-type: none"> <li>• Individual graphs that chart the performance metrics listed in the <b>Interface Statistics</b> dashlet</li> <li>• Interface availability</li> <li>• Top N QoS class map policy graph (inbound and outbound pre-policy rate, post-policy rate, and drops percentage)</li> <li>• QoS class map policy statistics (inbound and outbound)</li> </ul>
QoS	<p>For the selected QoS policy:</p> <ul style="list-style-type: none"> <li>• Summary information</li> <li>• Statistics and graphs for pre-policy, post-policy, and dropped class map traffic</li> <li>• Statistics and graphs for conforming, exceeding, and violating class map traffic</li> </ul>
IP SLA	<p>For Layer 3 services on the selected probe:</p> <ul style="list-style-type: none"> <li>• Summary information</li> <li>• IP Service Level Agreement (SLA) statistics</li> <li>• Delay, jitter, and frame loss between endpoints</li> <li>• Endpoint availability</li> </ul>

Dashboard Tab	Information Provided
Y1731	<p>For Layer 2 services on the selected probe:</p> <ul style="list-style-type: none"> <li>• Summary information</li> <li>• ITU-T Y.1731 statistics</li> <li>• Delay, jitter, and frame loss between endpoints</li> <li>• Endpoint availability</li> </ul> <p>At the bottom of this tab, dashlets list the endpoints with the highest values for the following parameters:</p> <ul style="list-style-type: none"> <li>• Delay (one- and two-way)</li> <li>• Jitter (one-way)</li> <li>• Frame loss</li> </ul>
BNG Statistics	<p>Broadband Network Gateway (BNG) information for the selected device:</p> <ul style="list-style-type: none"> <li>• Details such as its name, IP address, product type, and software version</li> <li>• Names of configured IP pools, as well as the number and percentage of available addresses used by each pool</li> <li>• Chart that graphs the number of used or free addresses for the selected IP pools</li> <li>• Charts that graph the number of sessions for authenticated and up subscribers by line card and session type</li> </ul> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• Use the check boxes below the charts to select the items you want to view information for</li> <li>• Place your cursor over any point in the graphs to view the values for the selected items at that particular time</li> </ul>



Dashboard Tab	Information Provided
ME1200 QoS	<p>Quality of Service (QoS) information for the selected service on a Cisco ME 1200 device:</p> <ul style="list-style-type: none"> <li>• Details such as the name of the device, the customer associated with this device, and its user-network interface (UNI) port.</li> <li>• Average bit and frame rates for green (conforming), yellow (exceeding), red (violating), and discard traffic. You can toggle between inbound and outbound traffic data.</li> <li>• Graphs that chart the traffic measured for the traffic types listed in the <b>ME1200 QoS Statistics</b> dashlet.</li> </ul> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• Five traffic graphs are provided: one for each traffic type as well as one consolidated graph.</li> <li>• You can toggle between viewing the data by frame rate (in frames per second) or bit rate (in kilobits per second).</li> <li>• You can specify the elements you want to view in a chart by checking the appropriate check box below that chart. In the consolidated traffic dashlet, you can specify traffic types. And in the individual traffic dashlets, you can specify one or multiple EVC Control Entries (ECEs) associated with the service.</li> </ul>
Optical SFPs	<p>For the selected Small Form-Factor Pluggable (SFP) Transceiver Module interface:</p> <ul style="list-style-type: none"> <li>• Details such as its name, the name and IP address of the device on which the interface is located, and its configured speed</li> <li>• The average, minimum, and maximum values for the following operating metrics: <ul style="list-style-type: none"> <li>• Optical input and output power</li> <li>• Operating temperature</li> <li>• Transceiver supply voltage</li> <li>• Laser bias current</li> </ul> </li> <li>• Individual graphs that chart the operating metrics listed in the <b>SFP Statistics</b> dashlet</li> </ul>

Dashboard Tab	Information Provided
SONET/TDM	<p>For the selected SONET or time-division multiplexing (TDM) interface:</p> <ul style="list-style-type: none"> <li>• Details such as its name, configured speed, and the IP address of the device it is located on</li> <li>• The average, minimum, and maximum values for the following performance metrics: <ul style="list-style-type: none"> <li>• Errored seconds</li> <li>• Severely errored seconds</li> <li>• C-bit severely errored seconds</li> <li>• P-bit severely errored seconds</li> <li>• Unavailable seconds</li> </ul> </li> </ul> <p>Values are provided for both the near-end (the receiving end) and far-end (the transmitting end) of the interface</p> <ul style="list-style-type: none"> <li>• Individual graphs that chart the performance metrics listed in the <b>SONET/TDM Statistics</b> dashlet</li> </ul>
Device Sensors	<p>For the sensors that reside on the selected device, details such as their name, the type of information they collect (such as temperature or voltage) and the corresponding unit of measure, and the value recorded during the last device poll.</p> <p><b>Note</b> Sensor data is not polled by default. To enable the collection of this data, create a monitoring policy based on the <b>Device Sensors</b> policy type (see <a href="#">Create a New Monitoring Policy Using Out-of-the-Box Policy Types</a>).</p>

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

## Network Summary Dashboard Overview

The **Network Summary** dashboard alerts you to the most important issues currently affecting your network. It also collects metrics from various sources to display a set of key performance indicators (KPIs). To open this dashboard, choose **Dashboard > Network Summary >** any of the tabs described in the following table.

Dashboard Tab	Information Provided
Network Devices	<ul style="list-style-type: none"> <li>• Status (ICMP reachability, SNMP reachability, device manageability), system health, and alarm summary metric dashlets</li> </ul> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• To open a pop-up window that describes the information provided by a metric dashlet, place your cursor over its name and then click the ? icon.</li> <li>• To open a page that lists the alarms or devices that correspond to a particular metric, click a dashlet value. For example, if the <b>SNMP Reachability Status</b> dashlet indicates that 50 devices are currently reachable via SNMP, click <b>50</b> to open the <b>Network Devices</b> page and view a listing of these devices.</li> </ul> <ul style="list-style-type: none"> <li>• Top N devices by CPU utilization, memory utilization, and environmental temperature</li> </ul> <p>For the <b>Top N Environmental Temperature</b> dashlet, note the following:</p> <ul style="list-style-type: none"> <li>• Two temperature values are provided for each device: its highest recorded internal temperature (displayed in the <b>Max Inlet Temp</b> column) and its highest recorded ambient temperature (displayed in the <b>Max Other Temp</b> column). By default, devices are sorted by their internal temperature.</li> <li>• To identify the sensor that recorded a particular temperature value, place your cursor over its <i>i</i> (<b>information</b>) icon.</li> </ul> <ul style="list-style-type: none"> <li>• Network topology</li> </ul>
Incidents	<ul style="list-style-type: none"> <li>• System health and alarm summary metric dashlets</li> </ul> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• To open a pop-up window that describes the information provided by a metric dashlet, place your cursor over its name and then click the ? icon.</li> <li>• To open a page that lists the alarms that correspond to a particular metric, click a dashlet value. For example, if the <b>Alarm Summary</b> dashlet indicates that 12 critical alarms have been raised in your network, click <b>12</b> to open the <b>Alarms</b> page and view a listing of these alarms.</li> </ul> <ul style="list-style-type: none"> <li>• Alarm count for the entire network and the Cisco EPN Manager server</li> <li>• Top N alarm types</li> <li>• Syslog summary</li> <li>• Top N event types and their count</li> <li>• Top N devices by number of syslogs sent</li> <li>• Syslog details such as the corresponding device, severity, and message text</li> <li>• Top N devices by number of alarms raised</li> </ul>

Dashboard Tab	Information Provided
Top N Interfaces	<p>For the selected port group:</p> <ul style="list-style-type: none"> <li>Interface availability and utilization summaries</li> <li>Top N devices by interface traffic, errors and discards, cyclic redundancy check (CRC) errors, and utilization</li> </ul> <p>Note the following:</p> <ul style="list-style-type: none"> <li>CRC error data is not polled by default. To enable the collection of this data, choose a polling frequency for the Interface Health monitoring policy's CRC parameter (see <a href="#">Change the Polling for a Monitoring Policy</a>).</li> <li>Due to a limitation in the current release, the Interface Health monitoring policy polls all of the interfaces in your network for CRC error data, not just the ones associated with the port group you chose from the <b>Port Groups</b> drop-down list. Keep this in mind when you view the data provided by the <b>Top N Interface CRC Errors</b> dashlet.</li> <li>Bottom N devices by interface availability</li> </ul> <p>Also note that the dashlets in this tab (except for the summary dashlets) allow you to open the 360 view for a device's adjacent device or interface by clicking its <b>i (information)</b> icon.</p>
Top N QoS	<p>For the selected port group:</p> <ul style="list-style-type: none"> <li>Top N devices by QoS pre-policy, post-policy, and drop rates</li> <li>Top N devices by conforming, exceeding, and violating traffic rates</li> </ul> <p>You can toggle between inbound and outbound traffic data.</p>

In the **Top N Interfaces** and **Top N QoS** tabs you can:

- Choose a specific device group and/or port group to view only information for those devices/ports.
  - To filter data for all the dashlets based on port/device groups, use the **Port Groups** filter at the top of the dashboard.
  - To filter data for a specific dashlet only, click the dashlet's **Edit** icon and choose a device/port group from the **Port Groups** and/or **Device Groups** drop-down list.
- Filter the data in the dashlets by Class Map (and you can choose to exclude the class-default).
- Click an interface's name link to view performance information for that interface in the **Performance** dashboard. If you click a link in the **Top N Interfaces** tab, the **Interfaces** tab opens. If you click a link in the **Top N QoS** tab, the **QoS** tab opens instead.
- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

## Cable Dashboard Overview

The **Cable** dashboard provides an executive overview of your cable network including the important issues currently affecting your network of Cisco cBR-8 devices. To open this dashboard, choose **Dashboard > Cable**.

Since Cable dashboards can provide both a high level overview and detailed insights of the cable network, dashboards are equipped with filter conditions that help in refining the displayed information.

- Filter information based on location or capabilities. The location you choose could be the group or location to which multiple devices are assigned.
- Filter information associated with a specific Cisco cBR-8 device.
- In addition to the above filters, the dashlets are interactive and can refine data further based on your need:
  - To refine the information provided in the table, you can do two things: First, you can create and apply a filter. And second, you can click a particular graph element. For example, in the **cBR-8 Dashboard** tab, if you click the bar that corresponds to a Cisco IOS XE version in the **Software Version** bar graph, the **Software Version Details** table only displays the information specific to that version.
  - Filters applied within a tab are applicable to all dashlets within the tab. For example, in the **Cable Modem** tab, if you filter a specific Cisco cBR-8 device, then all dashlets (such as **Modem Count by Vendors** and **Modem Count by Capability**) display information associated only with the filtered Cisco cBR-8 device.

The information provided in these tabs is refreshed periodically and can be configured through cable policies. To export the details displayed in the table rows as a .csv file, use the **Export** button.

### Before you begin:

To ensure that information is collected and reported for the Cisco cBR-8 routers in your network, verify that **Cable Policies** is listed on the **Monitoring Policies** page (**Monitor > Monitoring Tools > Monitoring Policies > Policies pane**), is currently active, and has polling intervals set for its parameters. To activate Cable monitoring policies, see, [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205](#).

Dashboard Tab	Information Provided
cBR-8 Dashboard	<p>Provides interactive graphs that chart the following metrics for the Cisco Converged Broadband Router-8 (cBR-8) routers in your network:</p> <ul style="list-style-type: none"> <li>• Software version—Indicates the number of routers (Cisco cBR-8 devices) running various Cisco IOS XE versions.</li> <li>• License usage—Indicates the number of license types applied to the selected routers.</li> <li>• License state—Indicates the number of routers with registered or unregistered licenses.</li> <li>• High availability (HA)—Indicates the number of routers configured with stateful switchover (SSO).</li> <li>• Remote physical device—Indicates the number of RPDs that are currently online, offline, establishing a connection with Cisco EPN Manager, or for whom deployment is pending.</li> <li>• Supervisor FPGA Versions—Indicates the field programmable gate arrays (FPGAs) currently in use, broken down by type and version.</li> </ul> <p>To view a table that provides additional information for one of these metrics, place your cursor over a metric and click anywhere within the resulting box that appears. For example, open the <b>High Availability Details</b> table and it provides information such as the name and IP address of Cisco cBR-8 routers, the amount of time they have been up, and the location of associated active and standby HA servers.</p> <p>You can also open a device's <b>Device 360</b> view by clicking its <i>i</i> (<b>information</b>) icon from the <b>Device IP</b> column.</p>
Cable Alarm	<p>Using interactive graphs for the alarms raised on Cisco cBR-8 routers in your network, the Alarm dashboard provides various statistics such as:</p> <ul style="list-style-type: none"> <li>• Alarm Severity: Indicates the number of alarms with different severity levels (Critical, Major, Minor, Warning, and Cleared).</li> <li>• Alarm Category: Indicates the number of alarms with a particular alarm category (such as CMTS System, CMTS Subscriber, Broadband Cable, etc.).</li> <li>• Group Location of Devices: Indicates the number of alarms raised on devices belonging to a different geographical locations.</li> <li>• cBR-8 Name: Group alarms raised on a specific cBR-8 device.</li> </ul> <p>You can filter alarms to view additional details about the alarm such as the alarm ID, failure source, time when the alarm was raised, the alarm protocol category, condition, and whether the alarm affects services. For more information about the alarm, use the Alarm ID hyperlink to navigate to the Alarms and Events page.</p> <p>In addition to various filters, the alarm heatmap provides a comprehensive count of alarms from various geographic locations and cBR-8 devices. The data is periodically refreshed and also updated based on your selection of the group location, device, or alarm severity.</p>

Dashboard Tab	Information Provided
Cable Modem	<p>Provides interactive graphs that chart the following metrics for cable modems associated with Cisco cBR-8 routers in your network:</p> <ul style="list-style-type: none"> <li>• Cable modem—Indicates the total count and operational states (such as Online, Offline, and Initializing) of available modems.</li> <li>• Modem count by vendors—Indicates the total number of online/offline cable modems from various vendors (such as Cisco Anis).</li> <li>• Modem count by capability—Indicates the total number of online cable modems with various DOCSIS versions (such as DOCSIS 1.1 and DOCSIS 2.0).</li> </ul> <p><b>Note</b> If you choose All (devices) in the filter option, only those devices associated with cable modems are filtered. The dashlets do not represent information about cable devices with no cable modems.</p>

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

## Device Trends Dashboard Overview

From the **Device Trends** dashboard, you can view performance information for a specific device, application, or service. To open this dashboard, choose **Dashboard > Device Trends >** any of the tabs described in the following table.

Dashboard Tab	Information Provided
Device	<p>For the selected device:</p> <ul style="list-style-type: none"> <li>• CPU utilization and memory utilization</li> <li>• Health information</li> <li>• Port summary</li> </ul>
Application	<p>For the selected application or service:</p> <ul style="list-style-type: none"> <li>• Traffic rate and volume</li> <li>• Top N clients, servers, and applications by traffic rate and volume</li> </ul>

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).

- For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

## DWDM/OTN Performance Dashboard Overview

From the **DWDM/OTN Performance** dashboard, you can view performance information for the dense wavelength division multiplexing (DWDM) and Optical Transport Network (OTN) interfaces in your network. This includes physical, optical data unit (ODU), optical transport unit (OTU), Ethernet, Synchronous Optical Network (SONET), and Synchronous Digital Hierarchy (SDH) interfaces. To open this dashboard, do one of the following:

- Choose **Dashboard > DWDM/OTN Performance > Optical Interface**.
- With an interface's 360 view open, choose **View > Performance**.

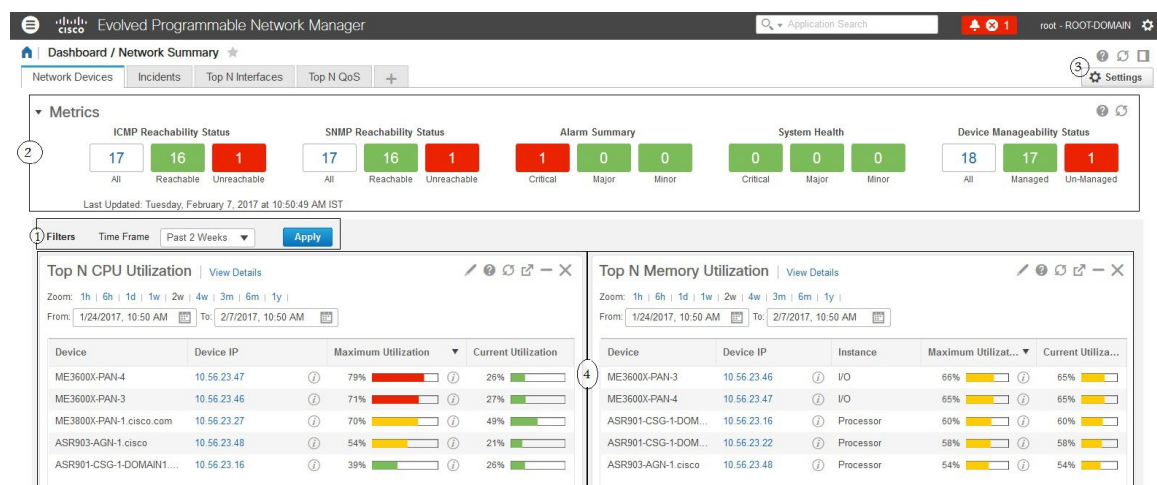
If you open the **DWDM/OTN Performance** dashboard using the first method, you also need to choose an interface from the **Interface** drop-down list. The dashlets provided by the dashboard will vary, depending on the type of interface you choose.

Note the following:

- The **Circuits** drop-down list is disabled, so you cannot use it to filter the information provided by this dashboard.
- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring](#), on page 198.
- For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

## How to Use the Dashboards

The following figure illustrates the key parts of a dashboard window and the controls you can use to adjust them.

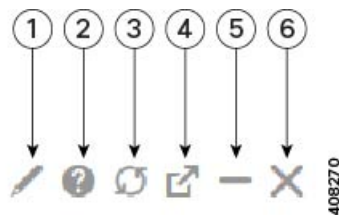




**Table 2: Dashboard Elements**

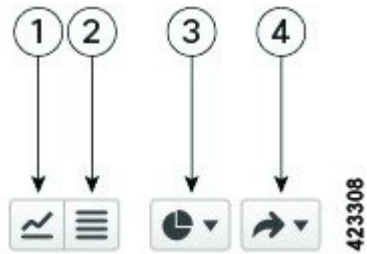
1	Dashboard filters—Filters all dashlets in the dashboard according to the selection. In this example, a time-based filter is used. The filters displayed depend on the dashboard type. For example, in the performance dashboards, you must select a specific interface, device, circuit, or VC.
2	Metric dashlets—Provides quick metrics for alarms, available devices, and so forth.
3	Dashboard settings and controls: <ul style="list-style-type: none"> <li>• Dashboard icons—Allows you to launch online help, refresh the entire dashboard, and open the <b>Dock</b> window.</li> <li>• Dashboard <b>Settings</b> menu—Allows you to add or rename a dashboard tab, add new dashlets (both standard and metric), adjust the dashboard's layout, reset all dashboards to their default settings, and export data from the selected dashlets.</li> </ul>
4	Standard dashlets—Provides at-a-glance data that is relevant to the dashboard.

In the top right corner of each dashlet are icons that are activated when you use that dashlet. The dashlet type determines the icons that are available. The most common icons are displayed in the following figure:



1	<b>Edit</b> icon—Click to change a dashlet's properties, such as its title, refresh interval, and the number of devices that are displayed (applicable only to Top N and Bottom N dashlets).
2	<b>Help</b> icon—Click to open a pop-up window that describes the dashlet, indicates the monitoring policy that needs to be activated in order for the dashlet to collect data, and lists the filters that can be applied to the dashlet.
3	<b>Refresh</b> icon: Click to refresh the information displayed in the dashlet.
4	<b>Detach</b> icon—Click to move the dashlet to another location in the dashboard.
5	<b>Collapse/Expand</b> icon—Click to toggle between a maximized and minimized dashlet.
6	<b>Close</b> icon—Click to remove the dashlet from the dashboard.

In the bottom right corner of dashlets that provide charts, you can find the buttons highlighted in the following figure. The buttons that are available will vary among dashlets.



1	<b>Chart View</b> button—Click to view a dashlet's information as a chart.
2	<b>Table View</b> button—Click to view a dashlet's information as a table.
3	<b>Chart Type</b> button—Click to choose the type of chart a dashlet displays (such as a bar or pie chart) and any options you want to set (such as displaying a unique fill pattern for each element).
4	<b>Actions</b> button—Click to print the information provided by a dashlet or export the information as either a .csv or .pdf format file.

See these topics for additional information on dashboards:

- [Types of Dashboards, on page 6](#)
- [Add Dashlets to Dashboards, on page 21](#)
- [Add a New Dashboard, on page 20](#)
- [Find Out Why Data Is Missing from a Dashboard](#)

## Add a New Dashboard

Use this procedure to create a new dashboard. Your new dashboard will appear as a new tab under one of the dashboards listed in [Types of Dashboards, on page 6](#).

<b>Step 1</b>	Open the relevant existing dashboard.  For example, if you want to create a new tab under the <b>Performance</b> dashboard, click any tab under <b>Dashboard &gt; Performance</b> .
<b>Step 2</b>	Click the + ( <b>Add New Dashboard</b> ) tab.  The <b>Settings</b> menu opens.
<b>Step 3</b>	Enter a name for the new dashboard, then click <b>Apply</b> .
<b>Step 4</b>	Click the new dashboard tab, then add dashlets as described in <a href="#">Add a Predefined Dashlet To a Dashboard, on page 21</a> .

## Customize a Dashboard Tab

To customize a tab in any of the dashboards that Cisco EPN Manager provides, complete the following procedure:

- 
- Step 1** Choose **Dashboard** > the dashboard tab you want to customize.
- For example, if you want to customize the **Performance** dashboard's **BNG** tab, you would choose **Dashboard** > **Performance** > **BNG**.
- Step 2** Adjust the dashboard tab as needed.
- You can do things like:
- Drag dashlets to a different location on the dashboard.
  - From the tab's **Settings** menu, rename a tab, add new dashlets (see [Add Dashlets to Dashboards](#)), and change the tab's layout.
- Note** To open a pop-up window that provides an overview of a dashlet you are thinking about adding, expand the **Add Dashlets** drop-down list, locate the dashlet, and then place your cursor over its name.
- Use the filters to specify the information you want to view and the appropriate time frame, then click **Apply**.
- Step 3** If necessary, troubleshoot why the tab is not displaying any data.
- See [Find Out Why Data Is Missing from a Dashboard](#) for more information.
- 

## Add Dashlets to Dashboards

You can add two types of dashlets to your dashboards:

- Prepackaged dashlets that are provided with Cisco EPN Manager —Some of the dashlets are displayed on dashboards by default; others are listed in the **Settings** menu, and you can add them as needed. These dashlets provide information you will likely monitor (for example, device CPU utilization, interface errors and discards, and traffic statistics). See [Add a Predefined Dashlet To a Dashboard](#), on page 21.
- Customized dashlets that you create to monitor device performance—These dashlet types can only be added to the **Device Trends** dashboard. See [Add a Customized Dashlet to the Device Trends Dashboard](#).

### Add a Predefined Dashlet To a Dashboard

Cisco EPN Manager provides a predefined set of dashlets that will provide you with commonly-sought network data. By default, a subset of these dashlets is already included in the dashboards, to help you get started. Complete the following procedure to add another of these predefined dashlets to your dashboards.




---

**Note** To edit or remove a dashlet, click the appropriate icon from the top right corner of that dashlet. (See [How to Use the Dashboards](#).)

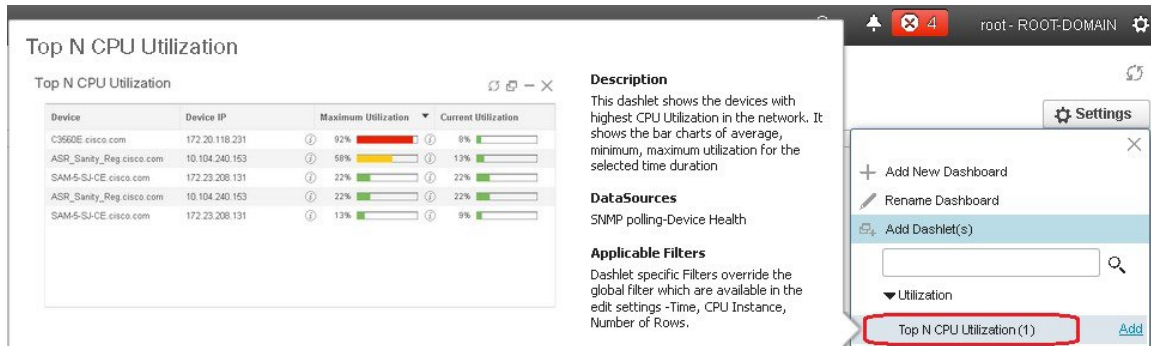
---

- 
- Step 1** From the sidebar menu, choose **Dashboard**, then select the dashboard you want to add a dashlet to.
- For example, to add a **Device Memory Utilization** dashlet to the **Device Trends** dashboard, choose **Dashboard** > **Device Trends** > **Device**.

## Add a Customized Dashlet to the Device Trends Dashboard

**Step 2** Identify the dashlet you want to add, then add it:

- From the top right corner of the dashboard, click **Settings** and then choose **Add Dashlets**. Cisco EPN Manager lists the dashlets that can be added to that dashboard.
- To open a pop-up window that provides an overview of a particular dashlet, place your cursor to the left of that dashlet's name. The pop-up window also lists the sources for the data the dashlet provides and the filters you can apply to the dashlet, as shown in the following illustration.



- Click **Add** to add the selected dashlet to the dashboard.

**Step 3** Verify that the dashlet is populated with data.

If it is not, check whether the required monitoring policy is enabled. (Only the Device Health monitoring policy is enabled by default. It checks device availability, CPU and memory pool utilization, and environmental temperature.)

- From the top right corner of the dashlet, click its **? (Help)** icon to open the dashlet's pop-up window.
- Check the information provided in the **Data Sources** area. If it lists a monitoring policy, check whether the policy is activated. See [Check What Cisco EPN Manager Is Monitoring, on page 198](#).

## Add a Customized Dashlet to the Device Trends Dashboard

If none of the dashlets in the **Device Trends** dashboard provide the device performance information you need, you can add a dashlet that uses a customized template to poll devices for their SNMP MIB attributes. Complete the following procedure to add this dashlet to the dashboard.

### Before you begin

Check the available monitoring policies to determine which policy collects the information you need. You will have to specify a policy during the dashlet creation process. If none of the policies meet your needs, you can create a policy that polls new parameters. See [Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 203](#).

**Step 1** Choose **Dashboard > Device Trends > Device**.

**Step 2** From the top right corner of the dashboard, click **Settings** and then choose **Add Dashlets**.

**Step 3** Expand the **Device Dashlets** list.

**Step 4** Locate **Generic Dashlet**, then click **Add**.

Cisco EPN Manager adds a blank generic dashlet to the **Device Trends** dashboard.

**Step 5** Configure the new dashlet as needed.

At a minimum, you should:

- Enter a meaningful title in the **Dashlet Title** field.
- Check the **Override Dashboard Time Filter** check box if you do not want to apply the time filters to all of the dashlets in the dashboard.
- In the **Type** drop-down list, choose whether the dashlet will display its data as a table or line chart. (Regardless of your choice, Cisco EPN Manager will display a toggle at the bottom of the dashlet that allows you to change the format.)
- In the **Policy Name** drop-down list, choose the monitoring policy that will collect the data for this dashlet. See [Monitoring Policies Reference, on page 767](#) for descriptions of the available monitoring policies.

**Step 6** Click **Save and Close**.

If no data is displayed in the dashlet, see [Find Out Why Data Is Missing from a Dashboard](#).

## Customize the Dock Window

Use the **Dock** window for quick navigation to frequently used web GUI pages and pop-up windows (such as the 360 view for a particular device). From here, you can also access links to the 15 most recently visited pages and Cisco EPN Manager training materials. To open this window, click the **Dock** icon (located in the top right area of the page).

Complete the following procedure to update the links provided in the **Dock** window:

**Step 1** Add a web GUI page link to the **Favorites** tab (**Dock icon > Links Visited > Favorites**):

- Open the web GUI page you want to add.
- Click its star (**Favorite**) icon, which is located in the top left area of the page.

**Step 2** Add a pop-up window link to the **Docked Items** area (**Dock icon > Docked Items**):

- Open the pop-up window you want to add, then open its 360 view.

- b) From the top right corner of the pop-up window, click the **Add to Dock** icon.
- 

## Find Out Why Data Is Missing from a Dashboard

If data is missing from a dashboard or dashlet, perform the following steps to identify the cause:

---

**Step 1** Check whether the dashlet data is filtered.

If you see **Edited** next to the dashlet name, do the following:

- a) Click the **Edit** icon and adjust the current filter settings.
- b) Click **Save and Close**.

**Step 2** Check whether there is a problem with the device.

See [Get Basic Device Information: Device 360 View, on page 63](#).

**Step 3** Check whether the device inventory is being collected properly.

See [Find Devices With Inventory Collection or Discovery Problems, on page 55](#).

**Step 4** Check whether Cisco EPN Manager is collecting the required data by viewing the monitoring policies it is using:

- a) Open the dashlet's overview pop-up window by clicking its **Help** icon.
- b) Note the monitoring policy listed under **Data Sources**.

Monitoring policies are described in [Monitoring Policies Reference, on page 767](#).

- c) Verify that this policy is listed and active in the **Monitoring Policies** page.

To open this page, choose **Monitor > Monitoring Tools > Monitoring Policies**, then choose **My Policies**.

- If the policy is not listed, proceed to Step 4d.
- If the policy is listed and its status is **Active**, click **Details** to open the **Collection Data** pop-up window and see if the device is being monitored by the policy. If it is not, you must adjust the policy as described in [Change the Device Set a Policy is Monitoring, on page 204](#). If the device is included in the policy, proceed to Step 5.
- If the policy is listed and its status is **Inactive**, select the policy and click **Activate**.

- d) Create a new monitoring policy and activate it.

See [Adjust What Is Being Monitored, on page 201](#).

**Step 5** Check whether the relevant data was purged from the system.

See [How Data Retention Settings Affect Web GUI Data, on page 663](#).


---

## Work In a Different Virtual Domain

Virtual domains are logical groupings of devices and are used to control your access to specific sites and devices. Virtual domains can be based on physical sites, device types, user communities, or any other designation the administrator chooses. All devices belong to ROOT-DOMAIN, which is the parent domain for

all new virtual domains. For more information about virtual domains, see [Create Virtual Domains to Control User Access to Devices, on page 682](#).

If you are allowed access to more than one virtual domain, you can switch to a different domain by completing the following procedure:

- 
- Step 1** Click  from the right side of the title bar.
- Step 2** Choose **Virtual Domain:** *current-domain*.
- Step 3** From the **Virtual Domain** drop-down list, choose a different domain.
- Cisco EPN Manager immediately changes your working domain.
- 

## Manage Jobs Using the Jobs Dashboard

If you have the appropriate user account privileges, you can manage Cisco EPN Manager jobs using the Jobs dashboard. To view the **Jobs** dashboard, choose **Administration > Dashboards > Job Dashboard**. From here, you can quickly see if a job was successful, partially successful, or failed.

If too many jobs are already running, Cisco EPN Manager will hold other jobs in the queue until resources are available. If this delays a scheduled job past its normal starting time, the job will not run. You will have to run it manually.

Some jobs may require approval. If this is the case, Cisco EPN Manager sends an email to users with Administrator privileges notifying them that a job was scheduled and needs approval. The job will only run after it is approved. See [Configure Job Approvers and Approve Jobs](#)

The following table describes the buttons displayed in the **Jobs** dashboard.

**Table 3: Jobs Dashboard Buttons**

Button	Description
<b>Delete Job</b>	Removes a job from the <b>Jobs</b> dashboard.
<b>Edit Job</b>	Edit the settings configured for the selected job.
<b>Edit Schedule</b>	Displays the series schedule and lets you edit it (start time, interval, and end time).
<b>Run</b>	Runs a new instance of the selected job. Use this to rerun partially successful or failed jobs; the job will only run for the failed or partially successful components.
<b>Abort</b>	Stops a currently-running job, but allows you to rerun it later. Not all jobs can be aborted; Cisco EPN Manager will indicate when this is the case.
<b>Cancel Series</b>	Stops a currently-running job and does not allow anyone to rerun it. If the job is part of a series, future runs are not affected.
<b>Pause Series</b>	Pauses a scheduled job series. When a series is paused, you cannot run any instances of that series (using <b>Run</b> ).

Button	Description
Resume Series	Resumes a scheduled job series that has been paused.



**Note** The **Delete Job**, **Abort**, and **Cancel Series** buttons are not available for system and poller jobs.

To view the details of a job, follow these steps:

- 
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
- Step 2** From the **Jobs** pane, choose a job series to get basic information (such as job type, status, job duration, and next start time).
- Step 3** To view the job interval, click a job instance hyperlink.
- At the top of the job page, the **Recurrence** field indicates how often the job recurs.
- Step 4** To get details about a failed or partially successful job, click the job instance hyperlink and expand the entries provided on the resulting page.
- This is especially helpful for inventory-related jobs. For example, if a user imported devices using a CSV file (a bulk import), the job will be listed in the **Jobs** sidebar menu under **User Jobs > Device Bulk Import**. The job details will list the devices that were successfully added and the devices that were not.
- 

### Example

To troubleshoot a failed software image import job:

1. Choose **User Jobs > Software Image Import** from the **Jobs** sidebar menu.
2. Locate the failed job in the table and then click its hyperlink.
3. Expand the job's details (if not already expanded) to view the list of devices associated with the job and the status of the image import for each device.
4. To view the import details for a specific device, click that device's *i* (**information**) icon in the **Status** column. This opens an **Image Management Job Results** pop-up window.
5. Examine each step and its status. For example, the **Collecting image with Protocol: SFTP** column might report that SFTP is not supported on the device.


## Extend Cisco EPN Manager Functions

Advanced users can extend Cisco EPN Manager using the following tools:

- Cisco Evolved Programmable Network Manager MTOSI API—Integrates Cisco EPN Manager with your operations support system (OSS).



- Cisco Evolved Programmable Network Manager REST API—Manages additional administrative operations.

To get information about these tools, click  from the right side of the title bar and then choose **Help > API Help**. You can also download the following documents from Cisco.com:

- [Cisco Evolved Programmable Network Manager MTOSI API Guide for OSS Integration](#)
- [Cisco Evolved Programmable Network Manager RESTCONF NBI Guide](#)

## Check Cisco.com for the Latest Cisco EPN Manager Documentation

Refer to the [Cisco Evolved Programmable Network Manager Documentation Overview](#) for information about and links to all of the documentation that is provided with Cisco EPN Manager .



---

**Note**

We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

---





## PART II

# Manage the Inventory

- [Add and Organize Devices, on page 31](#)
- [View Device Details, on page 63](#)
- [Manage Device Configuration Files, on page 91](#)
- [Manage Device Software Images, on page 107](#)
- [Perform Configuration Audits Using Compliance, on page 133](#)





## CHAPTER 2

# Add and Organize Devices

---

- [Which Devices Are Supported by Cisco EPN Manager ?, on page 31](#)
- [Which Device Software Versions Are Supported by Cisco EPN Manager ?, on page 32](#)
- [How Is Inventory Collected?, on page 33](#)
- [Configure Devices So They Can Be Modeled and Monitored, on page 34](#)
- [Apply Device Credentials Consistently Using Credential Profiles, on page 42](#)
- [Add Devices to Cisco EPN Manager , on page 44](#)
- [Check a Device's Reachability State and Admin Status, on page 52](#)
- [Move a Device To and From Maintenance State, on page 53](#)
- [Validate Added Devices and Troubleshoot Problems, on page 54](#)
- [Export Device Information to a CSV File, on page 55](#)
- [Create Groups of Devices for Easier Management and Configuration, on page 55](#)
- [Delete Devices, on page 62](#)


## Which Devices Are Supported by Cisco EPN Manager ?

[Cisco Evolved Programmable Network Manager Supported Devices](#) provides complete information about items such as:

- Supported device types and their sysObjectIDs
- Supported device software versions (see [Which Device Software Versions Are Supported by Cisco EPN Manager ?, on page 32](#))
- Supported inventory elements, such as modules, ports, and interfaces (physical and logical)
- Supported device configuration tasks (interfaces, routing protocols, and so forth)
- Supported configuration file archiving and software image management features
- Supported monitoring areas, such as device and interface health, reachability and availability, performance, and technology-specific monitoring
- Supported topology features, such as LLDP and CDP
- Supported MIBs used by monitoring policies

The table also provides information about all new support that is provided in Cisco EPN Manager maintenance packs.

Use either of these methods to view the device support table:

- From the web GUI—Click  at the top right corner of the window and choosing **Help > Supported Devices**.
- From Cisco.com—See [Cisco Evolved Programmable Network Manager Supported Devices](#).


**Note**

For the most current information, use the table that is on [Cisco.com](#).

## Which Device Software Versions Are Supported by Cisco EPN Manager ?

All devices should be running a *certified* device software version. However, certain devices must be running the *minimum* device software version. Follow the instructions in the table below on how to find out about a device software version.

Cisco EPN Manager may report that a device is running an *uncertified* device software version. You will likely notice no differences in how Cisco EPN Manager manages devices running an uncertified device software version. It depends on whether the device software version contains fundamental changes (changes to XML interfaces, SNMP commands, MIBs, CLI commands, and so forth). In some cases, Cisco EPN Manager will recognize the device software version but may not provide full support for the device NEs such as new modules.

To find this information:	Do the following:
A list of all certified device software versions	Refer to <a href="#">Cisco Evolved Programmable Network Manager Supported Devices</a> .
	Choose <b>Help &gt; Supported Devices</b> and hover over the "i" in the <b>Software Version</b> column to display a popup.
If a managed device is running an uncertified device software version	Choose <b>Monitor &gt; Managed Elements &gt; Network Devices</b> , locate the device, and hover your cursor over the "i" in the <b>Last Inventory Collection</b> column. Check if the popup displays <b>Uncertified Software Version</b> .
	From the device's Device Details page, under the Device Details tab, choose <b>System &gt; Summary</b> . Check if the Inventory area displays <b>[Uncertified Software Version]</b> .
Devices that require a minimum device software version	Choose <b>Help &gt; Supported Devices</b> and check the <b>Software Version</b> column for text similar to <b>&gt;=x.x</b> (For example, <b>&gt;=12.2</b> would indicate that the device must run at least device software version 12.2).

# How Is Inventory Collected?

After devices are added and discovered, Cisco EPN Manager will collect physical and logical inventory information and save it to the database. The following table describes how inventory collection is triggered.

Inventory Collection Trigger	Description
In response to incoming events	<p>Cisco EPN Manager receives an incoming NE SNMP trap, syslog, or TL1 message that signals a change on the NE. These incoming events include:</p> <ul style="list-style-type: none"> <li>• Configuration change events that signal a change in the device configuration. These events are normally syslogs or traps.</li> <li>• Other inventory events, such as tunnel up/down, link up/down, module in/out, and so forth.</li> </ul> <p>Cisco EPN Manager reacts to these incoming events by collecting NE inventory and state information to make sure that information in its database conforms to that of the NE. Most events trigger granular inventory collection, where Cisco EPN Manager only collects data relevant to the change event; other events will trigger a complete collection (sync) of the NE physical and logical inventory. The data that Cisco EPN Manager collects is determined by information in the incoming event, along with metadata that is defined in Cisco EPN Manager. The metadata in Cisco EPN Manager uses a combination of mechanisms—expedited events, reactive inventory, and granular polling—to fine-tune what is collected.</p> <p>For example, if Cisco EPN Manager receives a GMPLS Tunnel State Change event, it will collect ODU tunnel inventory information to discover midpoints and the Z endpoint of the tunnel.</p>
On demand	<p>Users can perform an immediate inventory collection (called <i>Sync</i>) from:</p> <ul style="list-style-type: none"> <li>• Network Devices page—Select one or more devices (by checking check boxes) and click <b>Sync</b>.</li> <li>• Device 360 view—Choose <b>Actions</b> &gt; <b>Sync Now</b>.</li> </ul> <p>See <a href="#">Collect a Device's Inventory Now (Sync)</a>, on page 269.</p>
Scheduled (daily)	<p>Normal inventory collection is usually performed overnight. Users with sufficient privileges can check when inventory is collected and the status of collection jobs by choosing <b>Administration</b> &gt; <b>Dashboards</b> &gt; <b>Job Dashboard</b> and choosing <b>System Jobs</b> &gt; <b>Inventory and Discovery Jobs</b>.</p>

## Enable archive logging on devices

Follow these steps to enable archive logging on devices so that granular inventory can be enabled for those devices on Cisco EPN Manager :

### For Cisco IOS-XR devices:

```
logging <epnm server ip> vrf default severity alerts
```

```
logging <epnm server ip> vrf default severity critical
logging <epnm server ip> vrf default severity error
logging <epnm server ip> vrf default severity warning
logging <epnm server ip> vrf default severity notifications
logging <epnm server ip> vrf default severity info
snmp-server host <epnm server ip> traps version 2c public
```

#### For Cisco IOS-XE devices:

```
logging host <epnm server ip> transport udp port 514
logging host <epnm server ip> vrf Mgmt-intf transport udp port 514
snmp-server host <epnm server ip> traps version 2c public
```

## Configure Devices So They Can Be Modeled and Monitored

- [Configure Devices To Forward Events To Cisco EPN Manager](#) , on page 34
- [Required Settings—Cisco IOS Device Operating System](#), on page 35
- [Required Settings—Cisco IOS XE Device Operating System](#), on page 35
- [Required Settings—Cisco IOS XR Device Operating System](#), on page 36
- [Required Settings—Cisco NCS Series Devices](#), on page 37
- [Required Settings—Cisco ONS Device Operating System](#), on page 42
- [Required Configuration for IPv6 Devices](#), on page 42




---

**Note** For information on the supported configuration of different device families, see, [Cisco Evolved Programmable Network Manager Supported Devices](#).

---

## Configure Devices To Forward Events To Cisco EPN Manager

To ensure that Cisco EPN Manager can query devices and receive events and notifications from them, you must configure devices to forward events to the Cisco EPN Manager server. For most devices, this means you must configure the devices to forward SNMP traps and syslogs.

For other devices (such as some optical devices), it means you must configure the devices to forward TL1 messages.

If you have a high availability deployment, you must configure devices to forward events to both the primary and secondary servers (unless you are using a virtual IP address; see [Using Virtual IP Addressing With HA](#), on page 728).

In most cases, you should configure this using the **snmp-server host** command. Refer to the topics in this document that list the prerequisites for the different device operating systems.




---

**Note** For information on the required configuration for enabling granular inventory on devices, see, [Cisco Evolved Programmable Network Manager Supported Syslogs](#) .

---



## Required Settings—Cisco IOS Device Operating System

```
snmp-server host server_IP
snmp-server community public-cmt RO
snmp-server community private-cmt RW
snmp-server ifindex persist
```

Do not change the device's default packet size (which is 1500 bytes). SNMP requests are sent in bulk by default. A small packet size could result in truncated responses.

The following setting disables domain lookups (which can cause Telnet command delays):

```
no ip domain-lookup
```

The following **syslog** settings are required.

```
logging server_IP
logging on
logging trap informational
logging buffered 64000 informational
logging event link-status default
```

The following **syslog** settings are required if the device has a management IP address (*interface\_name* is the active management IP address):

```
logging source-interface interface_name
```

## Required Settings—Cisco IOS XE Device Operating System

```
snmp-server host server_IP
snmp-server community public-cmt RO
snmp-server community private-cmt RW
snmp-server ifindex persist
```

Do not change the device's default packet size (which is 1500 bytes). SNMP requests are sent in bulk by default. A small packet size could result in truncated responses.

This setting disables domain lookups (which can cause Telnet command delays):

```
no ip domain-lookup
```

The following **syslog** settings are required.

```
logging server_IP
logging on
logging trap informational
logging buffered 64000 informational
logging event link-status default
```

The following syslog is required if the device has a management IP address (*interface\_name* is the active management IP address):

```
logging source-interface interface_name
```

## Required Settings—Cisco IOS XR Device Operating System



### Attention

If you are using Cisco NCS 4000 Series devices, do *not* complete the steps in this topic. Instead, complete the steps described in [Required Settings—Cisco NCS 4000 Series Devices, on page 38](#)

```
line default
no cli whitespace completion
snmp-server host server_IP
domain ipv4 host server_name server_IP
telnet ipv4 server max-servers no-limit
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist
vty-pool default 0 99
xml agent tty
netconf agent tty
service timestamps log datetime show-timezone msec year
telnet vrf default ipv4 server max-servers 100
```

Do not change the device's default packet size (which 1500 MB). SNMP requests are sent in bulk by default. A small packet size could result in truncated responses.

In addition to the required settings, you must follow these guidelines:

- Install the Cisco IOS XR Manageability Package (MGBL) on top of the Cisco IOS XR version. You can get information on this package from the release notes for your Cisco IOS XR version.
- Use the device login user that is a member of group **root-system** and **cisco-support**.
- User should use the admin user unique Telnet login *user@admin* (and also be a member of groups **root-system** and **cisco-support**).
- The devices must have one of the following SNMP community privileges: **SDROwner**, **SystemOwner** or the default (which means no specific level was specified). You may configure this as needed, using the following guidelines. (The following command is one line.)
- The SNMP and Telnet timeout values can be increased to 300 seconds using the Cisco EPN Manager GUI (Add Devices page).

```
snmp-server community [clear | encrypted] community-string [view view_name] [RO | RW]
[SDROwner | SystemOwner] [access_list_name]
```

The snmp-server command takes the following arguments.

Argument	Description
[ <b>clear</b>   <b>encrypted</b> ] <i>community-string</i>	Specifies the community-string command format and how it should be displayed in the <b>show running</b> command output: <ul style="list-style-type: none"> <li>clear — community-string is clear text and should be encrypted when displayed by <b>show running</b></li> <li>encrypted — community-string is encrypted text and should be displayed as such by <b>show running</b></li> </ul>
[ <b>view</b> <i>view-name</i> ]	Specifies the previously-defined view <i>view-name</i> which defines the objects available to the community
[ <b>SDROwner</b>   <b>SystemOwner</b> ]	Controls what Cisco EPN Manager users can see in web GUI: <ul style="list-style-type: none"> <li>SDROwner—Limits access to the Service Domain Router (SDR) owner. In other words, user will be able to view SDR owner modules and ports and SDR child modules. But the user will not be able to see the contents under SDR child modules and utility cards, such as fans, power supplies, and so forth.</li> <li>SystemOwner—Does not limit access. Users will be able to see the entire physical inventory (including utility cards) in the web GUI.</li> </ul>
[ <i>access-list-name</i> ]	List that contains IP addresses that are allowed to use community-string to access the SNMP agent.

The following syslog settings are also required.

```
logging server_IP
logging on
logging trap informational
logging facility local7
logging events level informational
logging events link-status software-interfaces
```

In the following **syslog** setting, the range indicates the minimum of 307200 and maximum of 125000000 log messages that can be stored on the device.

```
logging buffered <307200-125000000>
```

This syslog is required if the device has a management IP address (*interface\_name* is the active management IP address):

```
logging source-interface interface_name
```

If the device was added using its virtual IP address, configure it as follows:

```
ipv4 virtual address use-as-src-addr
```

## Required Settings—Cisco NCS Series Devices

- [Required Settings—Cisco NCS 4000 Series Devices, on page 38](#)

- [Required Settings—Cisco NCS 4200 Series Devices, on page 40](#)

## Required Settings—Cisco NCS 4000 Series Devices



### Attention

Ensure that both the MPLS and K9 packages are installed on the device before completing the following steps.

- Cisco EPN Manager uses SSH to secure communication with Cisco NCS 4000 series devices. To enable SSH, apply the following configuration settings on the device:

```
ssh server v2
ssh server rate-limit 600
```

- In MPLS traffic engineering configuration mode, enable event logging:

```
mpls traffic-eng logging events all
```

- Set the VTY options:

```
line default
exec-timeout 10 0
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

- Configure the Netconf and XML agents:

```
xml agent tty
netconf agent tty
```

- Configure SNMP on the device:

```
snmp-server host server_IP
snmp-server community public RO SystemOwner
snmp-server community private RW SystemOwner
snmp-server ifindex persist
```

You can use either SNMPv2 or SNMPv3:

- For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

- For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server group Group v3 priv notify Group read Group
```

For configuring the polling and configuration view, choose one of the following configuration options:

- SNMPv3 default configuration (used for SNMPv3 polling and viewing of the default configuration):

```
snmp-server group Group v3 priv read vldefault write vldefault notify vldefault
```

- SNMPv3 specific configuration:

- For SNMPv3 polling only:

```
snmp-server group Group v3 priv
```

- For viewing configuration for SNMPv3 set, polling, and for traps/informs notifications:

```
snmp-server group Group v3 priv notify epnm read epnm write epnm
```

- For viewing SNMPv3 - LLDP MIB OID configuration:

```
snmp-server view Group 1.0.8802.1.1.2 included
```




---

**Note** In the first line, *User* and *Group* are two distinct variables that you need to enter values for.

---

- Configure the stats command to improve the SNMP interface stats response time using the configuration

```
Snmp-server ifmib stats cache
```

- Configure SNMP traps for virtual interfaces to ensure that link-down scenarios are captured:

```
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
```

- Syslogs are used by Cisco EPN Manager for alarm and event management. NTP settings ensure that Cisco EPN Manager receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging Server_IP vrf name
```

Note the following:

- When specifying the time zone, enter the time zone's acronym and its difference (in hours) from Coordinated Universal Time (UTC). For example, to specify the time zone for a device located in Los Angeles, you would enter `clock timezone PDT -7`.
- Replace *Server\_IP* with the IP address of the host Cisco EPN Manager is installed on.

- Configure the Virtual IP address:

```
ipv4 virtual address NCS4K_Virtual_IP_Address/Subnet_Mask
ipv4 virtual address use-as-src-addr
```




---

**Note** *NCS4K\_Virtual\_IP\_Address* and *Subnet\_Mask* are two distinct variables separated by a slash. Be sure to enter a value for both of these variables.

---

- Enable performance management on all optical data unit (ODU) controllers:

### Example: Cisco NCS 4000 Device Settings

```
controller oduX R/S/I/P
per-mon enable
```

- Enable event logging of link status messages for optics controllers of Cisco NCS4000 devices running Cisco IOS release 6.1.42 or later:

```
controller Optics <x/y/z/w>
logging events link-status
```

- Enable performance management for Tandem Connection Monitoring (TCM):

```
tcm id {1-6}
perf-mon enable
```

- Configure the Telnet or SSH rate limit for accepting service requests:

- For Telnet, set the number of requests accepted per *second* (between 1-100; the default is 1):

```
cinetd rate-limit 100
```

- For SSH, set the number of request accepted per *minute* (between 1-600; the default is 60):

```
ssh server rate-limit 600
```

- To open Cisco Transport Controller (CTC) from Cisco EPN Manager (from a Device 360 view), enable the HTTP/HTTPS server:

```
http server ssl
```

- If you plan to use the Configuration Archive feature, devices must be configured as *secured*. To do this from CTC:

1. Choose **Provisioning > Security > Access**

2. Set EMS Access to **secure**.

- If you notice any performance issues because multiple Cisco NCS 4000 Series devices are sending information simultaneously, increase the number of Telnet sessions per *second*:

```
cinetd rate-limit 100
```

### Example: Cisco NCS 4000 Device Settings

This example configures Telnet on a Cisco NCS 4000 device using the VRF option, with no timeout:

```
telnet vrf default ipv4 server max-servers 1-100
vty-pool default 0 99 line-template default
line default
exec-timeout 0 0
```

## Required Settings—Cisco NCS 4200 Series Devices

- Cisco EPN Manager uses SSH to secure communication with Cisco NCS 4200 series devices. To enable SSH, apply one the following configuration settings on the device:

- enable
 

```
configure terminal
hostname name
ip domain-name name
crypto key generate rsa
```

- enable  
configure terminal  
ip ssh rsa keypair-name keypair-name  
crypto key generate rsa usage-keys label key-label modulus modulus-size  
ip ssh version [1 | 2]

- Set the VTY options:

```
line vty <#>
exec-timeout
session-timeout
transport input ssh
transport output ssh
```

- Configure SNMP on the device:

```
snmp-server host server_IP
snmp-server community public RO
snmp-server community private RW
```

You can use either SNMPv2 or SNMPv3:

- For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO
```

- For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha Password priv des Password
snmp-server view Group 1.3.6 included
snmp-server group Group v3 priv notify Group
```

For configuring the polling and configuration view, choose one of the following configuration options:

- SNMPv3 default configuration (used for SNMPv3 polling and viewing of the default configuration):

```
snmp-server group Group v3 priv read vldefault write vldefault notify vldefault
```

- SNMPv3 specific configuration:

- For SNMPv3 polling only:

```
snmp-server group Group v3 priv
```

- For viewing configuration for SNMPv3 set, polling, and for traps/informs notifications:

```
snmp-server group Group v3 priv notify epnm read epnm
```

- For viewing SNMPv3 - LLDP MIB OID configuration:

```
snmp-server view Group 1.0.8802.1.1.2 included
```




---

**Note** In the first line, *User* and *Group* are two distinct variables that you need to enter values for.

---

- Configure the cache settings at a global level to improve the SNMP interface response time using the configuration `Snmp-server cache`

- Syslogs are used by Cisco EPN Manager for alarm and event management. NTP settings ensure that Cisco EPN Manager receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging Server_IP vrf default severity info [port default]
mpls traffic-eng logging events all
mpls traffic-eng logging lsp setups
mpls traffic-eng logging lsp teardowns
```

Note the following:

- When specifying the time zone, enter the time zone's acronym and its difference (in hours) from Coordinated Universal Time (UTC). For example, to specify the time zone for a device located in Los Angeles, you would enter `clock timezone PDT -7`.
- Replace `Server_IP` with the IP address of the host Cisco EPN Manager is installed on.

## Required Settings—Cisco ONS Device Operating System

If you plan to use the Configuration Archive feature, devices must be configured as *secured*. You can do this from CTC:

1. From CTC, choose **Provisioning > Security > Access**.
2. Set EMS Access to secure.

## Required Configuration for IPv6 Devices

If you want to access a device that uses IPv6 addresses, configure the IPv6 address and static route on the Cisco EPN Manager server (virtual machine) by performing these steps:

1. Remove the ipv6 address autoconfig from the interface.
2. Configure the IPv6 address on the Cisco EPN Manager server.
3. Add a static route to the Cisco EPN Manager server.

## Apply Device Credentials Consistently Using Credential Profiles

Credential profiles are collections of device credentials for SNMP, Telnet/SSH, HTTP, and TL1. When you add devices, you can specify the credential profile the devices should use. This lets you apply credential settings consistently across devices.

If you need to make a credential change, such as changing a device password, you can edit the profile so that the settings are updated across all devices that use that profile.

To view the existing profiles, choose **Inventory > Device Management > Credential Profiles**.



## Create a New Credential Profile

Use this procedure to create a new credential profile. You can then use the profile to apply credentials consistently across products, or when you add new devices.

- 
- Step 1** Select **Inventory > Device Management > Credential Profiles**.
- Step 2** If an existing credential profile has most of the settings you need, select it and click **Copy**. Otherwise, click **Add**.
- Step 3** Enter a profile name and description. If you will have many credential profiles, make the name and description as informative as possible because that information will be displayed on the Credential Profiles page.
- Step 4** Enter the credentials for the profile. When a device is added or updated using this profile, the content you specify here is applied to the device.
- The SNMP read community string is required.
- Step 5** Click **Save Changes**.
- 

## Apply a New or Changed Profile to Existing Devices

Use this procedure to perform a bulk edit of devices and change the credential profile the devices are associated with. This operation overwrites any existing association between a device and a credential profile. You can also use this operation to synchronize device configurations with the new settings.



---

**Note** Make sure the profile's credential settings are correct before following this procedure and selecting **Update and Sync**. That operation will synchronize the devices with the new profile.

---

- 
- Step 1** Configure the credential profile using one of these methods:
- Create a new credential profile by choosing **Inventory > Device Management > Credential Profiles**, and clicking **Add**.
  - Edit an existing profile by choosing **Inventory > Device Management > Credential Profiles**, selecting the profile, and clicking **Edit**.
- Step 2** When you are satisfied with the profile, choose **Inventory > Device Management > Network Devices**.
- Step 3** Filter and select all of the devices you want to change (bulk edit).
- Step 4** Click **Edit**, and select the new credential profile from the Credential Profile drop-down list.
- Step 5** Save your changes:
- **Update** saves your changes to the Cisco EPN Manager database.
  - **Update and Sync** saves your changes to the Cisco EPN Manager database, collects the device physical and logical inventory, and saves all inventory changes to the Cisco EPN Manager database.
-

## Delete a Credential Profile

This procedure deletes a credential profile from Cisco EPN Manager . If the profile is currently associated with any devices, you must disassociate them from the profile.

- 
- Step 1** Check whether any devices are using the profile.
- Go to **Inventory > Device Management > Credential Profiles**.
  - Select the credential profile to be deleted.
  - Click **Edit**, and check if any devices are listed on the Device List page. If any devices are listed, make note of them.
- Step 2** If required, disassociate devices from the profile.
- Go to **Inventory > Device Management > Network Devices**.
  - Filter and select all of the devices you want to change (bulk edit).
  - Click **Edit**, and choose **--Select--** from the Credential Profile drop-down list.
  - Disassociate the devices from the old profile by clicking **OK** in the warning dialog box.
- Step 3** Delete the credential profile by choosing **Inventory > Device Management > Credential Profiles**, selecting the profile, and clicking **Delete**.
- 

## Add Devices to Cisco EPN Manager

Cisco EPN Manager uses device, location, and port groups to organize elements in the network. When you view devices in a table or on a map (network topology), the devices are organized in terms of the groups they belong to. When a device is added to Cisco EPN Manager , it is assigned to a group named **Unassigned Group**. You can then move the device into the desired groups as described in [Create Groups of Devices for Easier Management and Configuration, on page 55](#).



**Note** To add a Cisco WLC to Cisco EPN Manager , make sure it does not have any unsupported Access Points (APs), otherwise Cisco EPN Manager will not discover any APs from that WLC.

**Table 4: Methods for Adding Devices**

Supported Methods for Adding Devices	See:
Add multiple devices by discovering the neighbors of a seed device using:	<a href="#">Add Devices Using Discovery, on page 45</a> .
• Ping sweep and SNMP polling (Quick Discovery)	• <a href="#">Run Quick Discovery, on page 47</a>
• Customized protocol, credential, and filter settings (useful when you will be repeating the discovery job)	• <a href="#">Run Discovery With Customized Discovery Settings, on page 47</a>
Add multiple devices using the settings specified in a CSV file	<a href="#">Import Devices Using a CSV File, on page 49</a> .

Supported Methods for Adding Devices	See:
Add a single device (for example, for a new device type)	<a href="#">Add Devices Manually (New Device Type or Series), on page 50</a>

These topics provide examples of how to add a Carrier Ethernet and an Optical device to Cisco EPN Manager :

- [Example: Add a Single Cisco NCS 2000 or NCS 4000 Series Device, on page 51](#)
- [Example: Add a Network Element as an ENE Using Proxy Settings, on page 51](#)

## Add Cisco ME1200 devices in Cisco EPN Manager

Follow these settings while adding Cisco ME1200 devices in Cisco EPN Manager :

- SNMP - Use the same SNMP settings as that of other devices.
- CLI - Ensure that the protocol setting is set to SSH2. Though the device can be reached via telnet using a port, it is recommended to use SSH protocol. If telnet is used, then the custom telnet port used must be 2323.
- HTTP - Ensure you specify the right http credentials.
- Remember that configuration changes to Cisco ME1200 devices are not automatically discovered by Cisco EPN Manager . After making a change, you must manually sync the device. To do this, select the required device (s) in the Network Devices table and click **Sync**.

## Add Devices Using Discovery

Cisco EPN Manager supports two discovery methods:

- Ping sweep from a seed device (Quick Discovery). The device name, SNMP community, seed IP address and subnet mask are required. This method is not supported for discovering optical devices. See [Run Quick Discovery, on page 47](#)
- Using customized discovery methods (Discovery Settings)—This method is recommended if you want to specify settings and rerun discovery in the future. If you want to discover optical devices, use this method. See [Run Discovery With Customized Discovery Settings, on page 47](#).



### Note

- If a discovery job rediscovers an *existing* device and the device's last inventory collection status is **Completed**, Cisco EPN Manager does *not* overwrite the existing credentials with those specified in the Discovery Settings. For all other statuses (on existing devices), Cisco EPN Manager overwrites the device credentials with those specified in the Discovery Settings.
- Service discovery might take longer than usual when a large number of devices is added during database maintenance windows. Therefore, we recommend that you avoid large-scale operations during the night and on weekends.
- Autonomous APs are filtered out of the discovery process to optimise the discovery time. You need to manually add Autonomous APs using Import Devices or Credential Profile.

The discovery process of a device is carried out in the sequence of steps listed below. As Cisco EPN Manager performs discovery, it sets the reachability state of a device, which is: Reachable, Ping Reachable, or Unreachable. A description of the states is provided in [Device Reachability and Admin States, on page 52](#).

1. Cisco EPN Manager determines if a device is reachable using ICMP ping. If a device is not reachable, its reachability state is set to **Unreachable**.
2. Server checks if SNMP communication is possible or not.
  - If a device is reachable by ICMP but its SNMP communication is not possible, its reachability state is set to **Ping Reachable**.
  - If a device is reachable by both ICMP and SNMP, its reachability state is **Reachable**.
3. Verifies the device's Telnet and SSH credentials. If the credentials fail, details about the failure are provided in the Network Devices table in the **Last Inventory Collection Status** column (for example, **Wrong CLI Credentials**). The reachability state is not changed.
4. Modifies the device configuration to add a trap receiver so that Cisco EPN Manager can receive the necessary notifications (using SNMP).
5. Starts the inventory collection process to gather all device information.
6. Displays all information in the web GUI, including whether discovery was fully or partially successful.

**Note**

When Cisco EPN Manager verifies a device's SNMP read-write credentials, the device log is updated to indicate that a configuration change has been made by Cisco EPN Manager (identified by its IP address).

## Verify SNMP Communication

Follow these steps if the reachability state of a device is set as **Ping Reachable**.

**Note**

For Cisco NCS 2000 devices, verify the TL1 credentials, in addition (or instead) of SNMP credentials.

- Step 1** Ensure that the credentials used by Cisco EPN Manager for device verification are correct.
- Step 2** Verify that SNMP is enabled on the device and that the SNMP credentials configured on the device match those configured on Cisco EPN Manager.
- Step 3** Check whether SNMP packets are being dropped due to configuration errors or due to your security settings (default behavior) in all the network devices that are participating in transporting SNMP packets between the managed devices and the Cisco EPN Manager server.

## Specify the Management IP Address Type (IPv4/IPv6) for Discovered Devices

For discovered dual-home (IPv4/IPv6) devices, specify whether you want Cisco EPN Manager to use IPv4 or IPv6 addresses for management IP addresses.

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **Inventory > Discovery**.
- Step 2** From the **IPv4/IPv6 Preference for Management Address** drop-down list, choose either **V4** or **V6**.
- Step 3** Click **Save**.
- 

## Run Quick Discovery

Use this method when you want to perform a ping sweep using a single seed device. Only the device name, SNMP community, seed IP address and subnet mask are required. If you plan to use the configuration management features, you must provide the protocol, user name, password, and enable password.

### Before you begin

See [Configure Devices So They Can Be Modeled and Monitored, on page 34](#) to make sure your devices are configured correctly.

- 
- Step 1** Choose **Inventory > Device Management > Discovery**, then click the **Quick Discovery** link at the top right of the window.
- Step 2** At a minimum, enter the name, SNMP community, seed IP address, and subnet mask.
- Step 3** Click **Run Now**.
- 

### What to do next

Click the job hyperlink in the **Discovery Job Instances** area to view the results.

## Run Discovery With Customized Discovery Settings

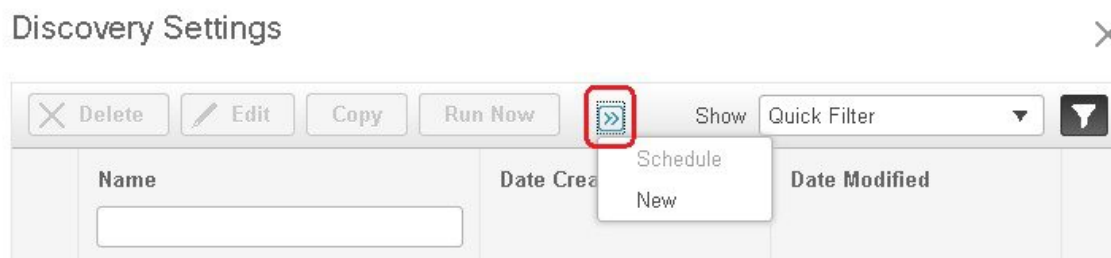
Cisco EPN Manager can discover network devices using discovery profiles. A discovery profile contains a collection of settings that instructs Cisco EPN Manager how to find network elements, connect to them, and collect their inventory. For example, you can instruct Cisco EPN Manager to use CDP, LLDP, OSPF to discover devices, or just perform a simple ping sweep (an example of the results of a ping sweep is provided in [Sample IPv4 IP Addresses for Ping Sweep, on page 48](#).) You can also create filters to fine-tune the collection, specify credential sets, and configure other discovery settings. You can create as many profiles as you need.

After you create a profile, create and run a discovery job that uses the profile. You can check the results of the discovery job on the Discovery page. You can also schedule the job to run again at regular intervals.

### Before you begin

See [Configure Devices So They Can Be Modeled and Monitored, on page 34](#) to make sure your devices are configured correctly so that Cisco EPN Manager can discover them.

- 
- Step 1** Choose **Inventory > Device Management > Discovery**, then click **Discovery Settings** at the top right of the window. (If you do not see a Discovery Settings link, click the arrow icon next to the Quick Discovery link.)
- Step 2** In the **Discovery Settings** popup, click **New**.
-



**Step 3** Enter the settings in the **Discovery Settings** window. Click "?" next to a setting to get information about that setting. For example, if you click "?" next to **SNMPv2 Credentials**, the help pop-up provides a description of the protocol and any required attributes.

**Step 4** Click **Run Now** to run the job immediately, or **Save** to save your settings and schedule the discovery to run later.

### Sample IPv4 IP Addresses for Ping Sweep

The following table provides an example of the results of a ping sweep.

Subnet Range	Number of Bits	Number of IP Addresses	Sample Seed IP Address	Start IP Address	End IP Address
255.255.240.0	20	4094	205.169.62.11	205.169.48.1	205.169.63.254
255.255.248.0	21	2046	205.169.62.11	205.169.56.1	205.169.63.254
255.255.252.0	22	1022	205.169.62.11	205.169.60.1	205.169.63.254
255.255.254.0	23	510	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.0	24	254	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.128	25	126	205.169.62.11	205.169.62.1	205.169.63.127
255.255.255.192	26	62	205.169.62.11	205.169.62.1	205.169.63.62
255.255.255.224	27	30	205.169.62.11	205.169.62.1	205.169.63.30
255.255.255.240	28	14	205.169.62.11	205.169.62.1	205.169.63.14
255.255.255.248	29	6	205.169.62.11	205.169.62.9	205.169.63.14
255.255.255.252	30	2	205.169.62.11	205.169.62.9	205.169.63.10
255.255.255.254	31	0	205.169.62.11		
255.255.255.255	32	1	205.169.62.11	205.169.62.11	205.169.62.11

### Example: Add Optical Devices Using Discovery

The following example shows how to use a seed device and the OTS protocol to discover Cisco NCS 2000 devices.

- 
- Step 1** Check [Configure Devices So They Can Be Modeled and Monitored, on page 34](#) to make sure the optical devices are configured correctly.
- Step 2** Choose **Inventory > Device Management > Discovery**, then click **Discovery Settings** at the top right of the window.
- Step 3** In the Discovery Settings window, click **New** to create a new discovery profile.
- Enter a discovery profile name—for example, **NCS2k\_3\_OTS**.
  - Enter the seed device and hop count information for the OTS protocol.
    - In the Protocol Settings area, click the arrow next to **Advanced Protocols** to open the discovery protocols list.
    - Click the arrow next to **OTS** to open the OTS protocol window.
    - Check the **Enable OTS** check box.
    - Click the Add Row ("+") icon.
    - Enter the seed device IP address and hop count (for example, **209.165.200.224** and **3**), then click **Save** to add the seed device information.
    - Click **Save** in the OTS protocol window to close the window. If necessary, click outside of the OTS Protocol window to close it.
  - Enter the TL1 device credentials for the Cisco NCS 2000 seed device.
    - In the Credential Settings area, click the arrow next to **TL1** to open the TL1 credentials window.
    - Check the **Enable TL1** check box.
    - Click the Add Row ("+") icon.
    - Enter the seed device IP address, username, password, and (if appropriate) proxy IP address .
    - For Secure TL1 access choose **Enable** from the **SSH** drop-down list, for Unsecured TL1 choose **Disabled**.
    - Click **Save** to add the credential information.
    - Click **Save** in the TL1 Credentials window to close the window. If necessary, click outside of the TL1 Credentials window to close it
- Step 4** Click **Save** to save the new discovery profile. The new **NCS2k\_3\_OTS** profile is added to the Discovery Settings window.
- Note** If you receive an error message, make sure you have enabled the protocols. (This is a common error.)
- Step 5** Select **NCS2k\_3\_OTS**, then click **Run Now** to begin the discovery job.
- Step 6** Check the results of the job by choosing **Inventory > Device Management > Discovery**.
- 

## Import Devices Using a CSV File

Use a CSV file to add devices if you have an existing management system from which you want to import devices, or you want to specify different values in a spreadsheet.

- [Create the CSV File, on page 49](#)
- [Import the CSV File, on page 50](#)

### Create the CSV File

Follow this procedure to create the CSV file.

- 
- Step 1** Create the bulk import CSV file using the template that is available from the Bulk Import dialog box. To open the dialog box, choose **Inventory > Device Management > Network Devices**, click the **+** icon above the Network Devices table, and choose **Bulk Import**. Use the **bulk device add sample template**.
- Step 2** To find out what the different fields mean and which fields are required, use the information that is in the web GUI. The information is the same for adding a single device or adding devices in bulk. To get this information, choose **Inventory > Device Management > Network Devices**, click the **+** icon above the Network Devices table, then choose **Add Device**. Mandatory fields are indicated by an asterisk; fields that require an explanation display a question mark next to them (hover your mouse cursor over the question mark to view the field details).
- Step 3** When you are done, save your changes and note the location of the file so you can import it as described in [Import the CSV File, on page 50](#).
- 

## Import the CSV File

Follow this procedure to import devices using a CSV file.

### Before you begin

See [Configure Devices So They Can Be Modeled and Monitored, on page 34](#) to make sure your devices are configured correctly.

- 
- Step 1** Choose **Inventory > Device Management > Network Devices**.
- Step 2** Click the **+** icon above the Network Devices table, then choose **Bulk Import**.
- Step 3** In the **Bulk Import** dialog:
- Make sure **Device** is chosen from the Operation drop-down list.
  - Click **Browse**, navigate to the CSV file, then click **Import**.
- Step 4** Check the status of the import by choosing **Administration > Dashboards > Job Dashboard**.
- Step 5** Click the arrow to expand the job details and view the details and history for the import job. If you encounter any problems, see [Validate Added Devices and Troubleshoot Problems, on page 54](#).
- 

## Add Devices Manually (New Device Type or Series)

Use this procedure to add a new device type and to test your settings before applying them to a group of devices.

### Before you begin

See [Configure Devices So They Can Be Modeled and Monitored, on page 34](#) to make sure your devices are configured correctly.

- 
- Step 1** Choose **Inventory > Device Management > Network Devices**.
- Step 2** Click the **+** icon above the Network Devices table, then choose **Add Device**.



- Step 3** In the **Add Device** dialog box, complete the required fields. Click the "?" next to a field for a description of that field.
- Note** Telnet/SSH information is mandatory for devices such as most Cisco NCS devices. . The following figure shows IPsec parameters to be configured.
- Step 4** (Optional) Click **Verify Credentials** to validate the credentials before adding the device.
- Step 5** Click **Add** to add the device with the settings you specified.
- 

## Example: Add a Single Cisco NCS 2000 or NCS 4000 Series Device

Cisco NCS 2000 series devices are TL1-based devices, and Cisco EPN Manager uses the TL1 protocol to communicate with these devices. Cisco NCS 4000 series devices, on the other hand, are Cisco IOS-XR devices, and Cisco EPN Manager uses the SNMP and Telnet/SSH protocols to communicate with these devices

---

- Step 1** Check [Configure Devices So They Can Be Modeled and Monitored, on page 34](#) to make sure the Cisco NCS devices are configured correctly.
- Step 2** Click the **+** icon above the Network Devices table, then choose **Add Device**.
- Step 3** In the **Add Device** dialog box, complete the required fields. Click the "?" next to a field for a description of that field.
- Cisco NCS 2000 series and Cisco ONS 15454—Enter TL1 parameters
  - Cisco NCS 4000 series—Enter SNMP and Telnet/SSH parameters
- Step 4** Click **Verify Credentials** to validate that Cisco EPN Manager can reach the device.
- Step 5** Click **Add** to add the device to Cisco EPN Manager .
- 

## Example: Add a Network Element as an ENE Using Proxy Settings

Messages sent to a particular network element must pass through other NEs in the network. To pass messages, one or more nodes can be a Gateway Network Element (GNE) and connect other NEs in your network. A node becomes a GNE when you establish a TL1 session and enter a command that must be sent to another node. The node that receives the TL1 message from another node for processing is an End-point Network Element (ENE). Messages from an ENE are transmitted through a GNE to other NEs in the network.

---

- Step 1** Check [Configure Devices So They Can Be Modeled and Monitored, on page 34](#) to make sure your devices are configured correctly.
- Step 2** Click the **+** icon above the Network Devices table, then choose **Add Device**.
- Step 3** In the **Add Device** dialog box, under the General Parameters, enter the IP address or the DNS name of the ENE that you want to add. Click the "?" next to a field for a description of that field.
- Step 4** Under the TL1 Parameters, enter the proxy IP address for the node that you are using as an ENE.
- Step 5** Click **Verify Credentials** to validate that Cisco EPN Manager can connect to the device.
- Step 6** Click **Add** to add the device to Cisco EPN Manager .
-

## Check a Device's Reachability State and Admin Status





Use this procedure to determine whether Cisco EPN Manager can communicate with a device (reachability state) and whether it is managing that device (admin status). The admin status also provides information on whether the device is being successfully managed by Cisco EPN Manager.

- 
- Step 1** Choose **Inventory > Device Management > Network Devices**.
- Step 2** Locate your device in the Network Devices table.
- From the **Show** drop-down list (at the top right of the table), choose **Quick Filter**.
  - Enter the device name (or part of it) in the text box under the **Device Name** column.
- Step 3** Check the information in the **Reachability** and **Admin Status** columns. See [Device Reachability and Admin States](#), on page 52 for descriptions of these states.
- 

## Device Reachability and Admin States





**Device Reachability State**—Indicates whether Cisco EPN Manager can communicate with the device using all configured protocols.

**Table 5: Device Reachability State**

Icon	Device Reachability State	Description	Troubleshooting
	Reachable	Cisco EPN Manager can reach the device using SNMP, or the NCS 2K device using ICMP.	—
	Ping reachable	Cisco EPN Manager can reach the device using Ping, but not via SNMP.	Although ICMP ping is successful, check for all possible reasons why SNMP communication is failing. Check that device SNMP credentials are the same in both the device and in Cisco EPN Manager, whether SNMP is enabled on the device, or whether the transport network is dropping SNMP packets due to reasons such as mis-configuration, etc. See <a href="#">Change Basic Device Properties</a> , on page 271.
	Unreachable	Cisco EPN Manager cannot reach the device using Ping.	Verify that the physical device is operational and connected to the network.
	Unknown	Cisco EPN Manager cannot connect to the device.	Check the device.

**Device Admin State**—Indicates the configured state of the device (for example, if an administrator has manually shut down a device, as opposed to a device being down because it is not reachable by Ping).

**Table 6: Device Admin State**

Icon	Device Admin State	Description	Troubleshooting
	Managed	Cisco EPN Manager is actively monitoring the device.	Not Applicable.
	Maintenance	Cisco EPN Manager is checking the device for reachability but is not processing traps, syslogs, or TL1 messages.	To move a device back to Managed state, see <a href="#">Move a Device To and From Maintenance State, on page 53</a> .
	Unmanaged	Cisco EPN Manager is not monitoring the device.	<p>In the Network Devices table, locate the device and click the "i" icon next to the data in the <b>Last Inventory Collection Status</b> column. The popup window will provide details and troubleshooting tips. Typical reasons for collection problems are:</p> <ul style="list-style-type: none"> <li>• Device SNMP credentials are incorrect.</li> <li>• The Cisco EPN Manager deployment has exceeded the number of devices allowed by its license.</li> <li>• A device is enabled for switch path tracing only.</li> </ul> <p>If a device type is not supported, its Device Type will be <b>Unknown</b>. You can check if support for that device type is available from Cisco.com by choosing <b>Administration &gt; Licenses and Software Updates &gt; Software Update</b> and then clicking <b>Check for Updates</b>.</p>
	Unknown	Cisco EPN Manager cannot connect to the device.	Check the device.

## Move a Device To and From Maintenance State

When a device's admin status is changed to Maintenance, Cisco EPN Manager will not poll the device for inventory changes, nor will it process any traps or syslogs that are generated by the device. However, Cisco EPN Manager will continue to maintain existing links and check the device for reachability.

See [Device Reachability and Admin States, on page 52](#) for a list of all admin states and their icons.

**Step 1** From the Network Devices table, choose **Admin State > Set to Maintenance State**.

**Step 2** To return the device to the fully managed state, choose **Admin State > Set to Managed State**.

---

## Validate Added Devices and Troubleshoot Problems

To monitor the discovery process, follow these steps:

---

**Step 1** To check the discovery process, choose **Inventory > Device Management > Discovery**.

**Step 2** Expand the job instance to view its details, then click each of the following tabs to view details about that device's discovery:

- **Reachable** - Devices that were reached using ICMP. Devices may be reachable, but not modeled, this may happen due to various reasons as discussed in [Add Devices Using Discovery, on page 45](#). Check the information in this tab for any failures.
- **Filtered** - Devices that were filtered out according to the customized discovery settings.
- **Ping Reachable** - Devices that were reachable by ICMP ping but could not be communicated using SNMP. This might be due to multiple reasons: invalid SNMP credentials, SNMP not enabled in device, network dropping SNMP packets, etc.
- **Unreachable** - Devices that did not respond to ICMP ping, with the failure reason.
- **Unknown** - Cisco EPN Manager cannot connect to the device by ICMP or by SNMP.

**Note** For devices that use the TL1 protocol, make sure that node names do not contain spaces. Otherwise, you will see a connectivity failure.

**Step 3** To verify that devices were successfully added to Cisco EPN Manager, choose **Inventory > Device Management > Network Devices**. Then:

- Verify that the devices you have added appear in the list. Click a device name to view the device configurations and the software images that Cisco EPN Manager collected from the devices.
- View details about the information that was collected from the device by hovering your mouse cursor over the Inventory Collection Status field and clicking the icon that appears.
- Check the Device Reachability Status and Admin Status columns. See [Device Reachability and Admin States, on page 52](#).

If you need to edit the device information, see [Change Basic Device Properties, on page 271](#).

To verify that Cisco EPN Manager supports a device, refer to [Cisco Evolved Programmable Network Manager Supported Devices](#).

To verify that Cisco EPN Manager supports a device, click the Settings icon (⚙️), then choose .

---

## Find Devices With Inventory Collection or Discovery Problems

Use the quick filter to locate devices that have discovery or collection problems.

- 
- Step 1** Choose **Monitor > Device Management > Network Devices** to open the Network Devices page.
- Step 2** Make sure **Quick Filter** is listed in the **Show** drop-down at the top left of the table.
- Step 3** Place your cursor in the quick filter field above the **Collection Status** and select a status from the drop-down list that is displayed. The devices are filtered according to that status. For troubleshooting steps, see [Validate Added Devices and Troubleshoot Problems, on page 54](#).
- 

## Export Device Information to a CSV File


When you export the device list to a file, all device information is exported into a CSV file. The file is then compressed and encrypted using a password you select. The exported file contains information about the device's SNMP credentials, CLI settings, and geographical coordinates. The exported file includes device credentials but does not include credential profiles.



---

**Caution** Handle the CSV file with care because it lists all credentials for the exported devices. You will want to ensure that only users with special privileges can perform a device export.

---

- 
- Step 1** Choose **Inventory > Device Management > Network Devices**.
- Step 2** Select the devices that you want to export, then click  and choose **Export Device**.
- Step 3** In the **Export Device** dialog box, enter a password that will be used to encrypt the exported CSV file. Users will need to supply this password to open the exported file.
- Step 4** Confirm the encryption password and click **Export**. Depending on your browser configuration, you can save or open the compressed file.
- 

## Create Groups of Devices for Easier Management and Configuration

- [How Groups Work, on page 56](#)
- [Create User-Defined Device Groups, on page 59](#)
- [Create Location Groups, on page 60](#)
- [Create Port Groups, on page 61](#)
- [Make Copies of Groups, on page 61](#)

- [Hide Groups That Do Not Have Any Members, on page 62](#)
- [Delete Groups, on page 62](#)

Organizing your devices into logical groupings simplifies device management, monitoring, and configuration. Because you can apply operations to groups, grouping saves time and ensures that configuration settings are applied consistently across your network. In smaller deployments where all devices can be configured with the same settings, you may only need to create one general device group. The grouping mechanism also supports subgroups. You will see these groups in many of the Cisco EPN Manager GUI windows.

When a device is added to Cisco EPN Manager, it is assigned to a location group named **Unassigned**. If you are managing a large number of devices, be sure to move devices into other groups so that the Unassigned Group membership does not become too large.

## How Groups Work

Groups are logical containers for network elements, such as devices and ports. You can create groups that are specific to your deployment—for example, by device type or location. You can set up a group so that new devices are automatically added if they match your criteria, or you may want to add devices manually.

For information on the specific types of groups, see the related topics [Network Device Groups, on page 56](#) and [Port Groups, on page 57](#).

For information on how elements are added to groups, see [How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups, on page 58](#).

## Network Device Groups

The following table lists the supported types of network device groups. The device groups can be accessed from the Inventory.

Network Device Group Type	Membership Criteria	Can Be Created or Edited By Users?
Device Type	<p>Devices are grouped by family (for example, Optical Networking, Routers, Switches and Hubs, and so forth). Under each device family, devices are further grouped by series. New devices are automatically assigned to the appropriate family and series groups. For example, a Cisco ASR 9006 would belong to Routers (family) and Cisco ASR 9000 Series Aggregation Services Routers (series).</p> <p>Note the following:</p> <ul style="list-style-type: none"> <li>• You cannot create a device type group; these are dynamic groups that are system-defined. Instead, use device criteria to create a user-defined group and give it an appropriate device name.</li> <li>• Device type groups are not displayed in Network Topology maps.</li> <li>• Unsupported devices discovered by Cisco EPN Manager are automatically assigned the <b>Generic Cisco Device</b> device type and are listed under <b>Device Type &gt; Generic Cisco Device Family</b>.</li> </ul>	No

Location	<p>Location groups allow you to group devices by location. You can create a hierarchy of location groups (such as theater, country, region, campus, building, and floor) by adding devices manually or by adding devices dynamically.</p> <p>A device should appear in one location group only, though a higher level “parent” group will also contain that device. For example, a device that belongs to a <i>building</i> location group might also indirectly belong to the parent campus group.</p> <p>By default, the top location of the hierarchy is the <b>All Locations</b> group. All devices that have not been assigned to a location appear under the Unassigned group under All Locations.</p>	Yes
User Defined	<p>Devices are grouped by a customizable combination of device and location criteria. You can customize group names and use whatever device and location criteria you need.</p>	Yes

## Port Groups

The following table lists the supported types of port groups.

Port Group Type	Membership Criteria	Can be created or edited by users?
Port Type	<p>Grouped by port type, speed, name, or description. Ports on new devices are automatically assigned to the appropriate port group.</p> <p>You cannot create Port Type groups. Instead, use device criteria to create a user-defined group, and create subgroups under the user-defined group.</p>	No; instead create a User Defined Group

System Defined	<p>Grouped by port usage or state. Ports on new devices are automatically assigned to the appropriate port group.</p> <p>Link Ports—Ports that are connected to another Cisco device or other network devices and are operating on “VLAN” mode and are assigned to a VLAN.</p> <p>Trunk Ports—Ports that are connected to a Cisco device or other network devices(Switch/Router/Firewall/Third party devices) and operating on “Trunk” mode in which they carry traffic for all VLANs.</p> <p>If the status of a port goes down, it is automatically added to Unconnected Port group. You cannot delete the ports in this group, and you cannot re-create this group as a sub group of any other group.</p> <p>Wireless and Data Center devices use the other System Defined port groups: AVC Configured Interfaces, UCS Interfaces, UCS Uplink Interfaces, WAN Interfaces, and so forth.</p> <p>You cannot create System Defined Port groups. Instead, use device criteria to create a user-defined group, and create subgroups under the user-defined group.</p>	No; instead create a User Defined Group
User Defined	Grouped by a customizable combination of port criteria, and you can name the group. If the group is dynamic and a port matches the criteria, it is added to the group.	Yes

## How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups

How elements are added to a group depends on whether the group is dynamic, manual, or mixed.

Method for Adding Devices	Description
Dynamic	Cisco EPN Manager automatically adds a new element to the group if the element meets the group criteria. While there is no limit to the number of rules that you can specify, the performance for updates may be negatively impacted as you add more rules.
Manual	Users add the elements manually when creating the group or by editing the group.
Mixed	Elements are added through a combination of dynamic rules and manual additions.

The device inheritance in parent-child user defined and location groups are as follows:

- User Defined Group—When you create a child group:
  - If the parent and child groups are both dynamic, the child group can only access devices that are in the parent group.
  - If the parent group is static and the child group is dynamic, the child group can access devices that are outside of the parent group.



- If the parent and child groups are dynamic and static, the child group "inherits" devices from the parent device group.
- Location Group—The parent group inherits the child group devices.

## Groups and Virtual Domains

While groups are logical containers for elements, access to the elements is controlled by virtual domains. This example shows the relationship between groups and virtual domains.

- A group named **SanJoseDevices** contains 100 devices.
- A virtual domain named **NorthernCalifornia** contains 400 devices. Those devices are from various groups and include 20 devices from the **SanJoseDevices** group.

Users with access to the **NorthernCalifornia** virtual domain will be able to access the 20 devices from the **SanJoseDevices** group, but not the other 80 devices in the group. For more details, see "Create Virtual Domains to Control User Access to Devices".

## Create User-Defined Device Groups

To create a new device type group, use the user-defined group mechanism. You must use this mechanism because device type groups are a special category used throughout Cisco EPN Manager. The groups you create will appear in the **User Defined** category.



**Note** Cisco ASR satellites can only belong to location groups. For more information, see [Satellite Considerations in Cisco EPN Manager](#), on page 234.

To create a new group, complete the following procedure:

- Step 1** Choose **Inventory > Group Management > Network Device Groups**.
  - Step 2** In the **Device Groups** pane, click the + (**Add**) icon and then choose **Create User Defined Group**.
  - Step 3** Enter the group's name and description. If other user-defined device type groups already exist, you can set one as the parent group by choosing it from the **Parent Group** drop-down list. If you do not select a parent group, the new group will reside in the **User-Defined** folder (by default).
  - Step 4** Add devices to the new group:
 

If you want to add devices that meet your criteria automatically, enter the criteria in the **Add Devices Dynamically** area. To group devices that fall within a specific range of IP addresses, enter that range in square brackets. For example, you can specify the following:

    - IPv4-10.[101-155].[1-255].[1-255] and 10.126.170.[1-180]
    - IPv6-2014::5217:[0000-ffff]:fe22:[1e40-1f41]
- Note** While there is no limit on the number of rules you can specify for a dynamic group, group update performance could become slower as the number of rules increases.

If you want to add devices manually, do the following:

1. Expand the **Add Devices Manually** area and then click **Add**.
2. In the **Add Devices** dialog box, check the check boxes for the devices you want to add, then click **Add**.

**Step 5** Click the **Preview** tab to see the members of your group.

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

The new device group appears in the folder you selected in Step 3.

## Create Location Groups



**Note** Cisco ASR satellites can only belong to Location Groups. For more information, see [Satellite Considerations in Cisco EPN Manager](#), on page 234.

To create a location group, follow these steps:

- Step 1** Choose **Inventory > Group Management > Network Device Groups**.
- Step 2** In the **Device Groups** pane on the left, click the **Add** icon, then choose **Create Location Group**.
- Step 3** Enter the name and description, and choose a group from the **Parent Group** drop-down list. By default, the group will be an All Locations subgroup (that is, displayed under the **All Locations** folder).
- Step 4** If you are creating a device group based on geographical location, for example, all devices located in a building at a specific address, select the Geographical Location check box and specify the GPS coordinates of the group or click the **View Map** link and click on the required location in the map. The GPS coordinates will be populated automatically in this case. Note that location groups defined with a geographic location are represented by a group icon in the geo map. The devices you add to the group will inherit the GPS coordinates of the group. See [Device Groups in the Geo Map](#), on page 176 for more information. Note that if geographical location is the primary reason for grouping a set of devices, it is recommended that the devices you add to the group do not have their own GPS coordinates that are different from the group's.
- Step 5** If you want devices to be added automatically if they meet certain criteria, enter the criteria in the **Add Device Dynamically** area. Otherwise, leave this area blank.  
  
While there is no limit on the number of rules that you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.
- Step 6** If you want to add devices manually:
  - a) Under **Add Devices Manually**, click **Add**.
  - b) In the **Add Devices** dialog box, locate devices you want to add, then click **Add**.
- Step 7** Click the **Preview** tab to see the group members.
- Step 8** Click **Save**, and the new location group appears under the folder you selected in Step 3 (**All Locations**, by default).

## Create Port Groups

To create a port group, follow these steps:

- 
- Step 1** Choose **Inventory > Group Management > Port Groups**.
- Step 2** From **Port Groups > User Defined**, hover your mouse over the "i" icon next to **User Defined** and click **Add SubGroup** from the popup window.
- Step 3** Enter the name and description, and choose a group from the **Parent Group** drop-down list. By default, the port group will be under the **User Defined** folder.
- Step 4** Choose the devices a port must belong to in order to be added to the group. From the **Device Selection** drop-down list, you can:
- **Device**—To choose devices from a flat list of all devices.
  - **Device Group**—To choose device groups (Device Type, Location, and User Defined groups are listed).
- Step 5** If you want ports to be added automatically if they meet your criteria, enter the criteria in the **Add Port Dynamically** area. Otherwise, leave this area blank.
- While there is no limit on the number of rules that you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.
- Step 6** If you want to add devices manually:
- a) Under **Add Ports Manually**, click **Add**.
  - b) In the **Add Ports dialog** box, locate devices you want to add, then click **Add**.
- Step 7** Click the **Preview** tab to see the group members.
- Step 8** Click **Save**, and the new port group appears under the folder you selected in Step 3 (**User Defined**, by default).
- 

## Make Copies of Groups

When you create a duplicate of a group, Cisco EPN Manager names the group **CopyOfgroup-name** by default. You can change the name, if required.

To duplicate a group follow these steps:

- 
- Step 1** Choose **Inventory > Group Management > Network Device Groups**.
- Step 2** Choose the group from the Device Groups pane on the left.
- Step 3** Locate the device group you want to copy, then click the "i" icon next to it to open the pop-up window.
- Step 4** Click **Duplicate Group** (do not make any changes yet) and click **Save**. Cisco EPN Manager creates a new group called **CopyOfgroup-name**.
- Step 5** Configure your group as described in [Create User-Defined Device Groups, on page 59](#) and [Create Location Groups, on page 60](#).
- Step 6** Verify your group settings by clicking the **Preview** tab and examining the group members.
- Step 7** Click **Save** to save the group.
-

## Hide Groups That Do Not Have Any Members

By default, Cisco EPN Manager will display a group in the web GUI even if the group has no members. Users with Administrator privileges can change this setting so that empty groups are hidden—that is, they are not displayed in the web GUI. (Hidden groups are not deleted from Cisco EPN Manager.)

---

**Step 1** Choose **Administration > Settings > System Settings**, then choose **Inventory > Grouping**.

**Step 2** Uncheck **Display groups with no members**, and click **Save**.

We recommend that you leave the **Display groups with no members** check box selected if you have a large number of groups and devices. Unselecting it can slow system performance.

---

## Delete Groups

Make sure the group you want to delete has no members, otherwise Cisco EPN Manager will not allow the operation to proceed.

---

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

**Step 2** Locate the device group you want to delete in the Device Groups pane on the left, then click the "i" icon next to it to open the pop-up window.

**Step 3** Click **Delete Group** and click **OK**.

---

## Delete Devices

When you delete a device, Cisco EPN Manager will no longer model or monitor it.

### Before you begin

If a device has services on it that were provisioned using Cisco EPN Manager, you must delete those services before deleting the device. However, you will be permitted to delete devices that have discovered or provisioned services on it (that is, services that were not created by Cisco EPN Manager). To find out which services are on a device, use the Device 360 view; see [View a Specific Device's Circuits/VCs, on page 534](#).

---

**Step 1** Choose **Inventory > Device Management > Network Devices** to open the Network Devices page.

**Step 2** Locate the device you want to delete. For example, navigate through the Groups list, or enter some text in the Quick Filter boxes.

**Step 3** Select the device, and click **Delete**.

---



## CHAPTER 3

# View Device Details

The following topics explain how to get more information about your network devices. You can also generate a variety of device reports that provide hardware and software details, CPU and memory utilization, general device health, and so forth. For information on these reports, see [Device Reports, on page 259](#). For information on inventory collection, see [How Is Inventory Collected?, on page 33](#).

- [Find Devices, on page 63](#)
- [Get Basic Device Information: Device 360 View, on page 63](#)
- [View a Device's Local Topology from the Device 360 View, on page 67](#)
- [View the Network's Hardware Inventory, on page 68](#)
- [Get Complete Device Information: Device Details Page, on page 68](#)
- [View and Manage Devices Using the Chassis View, on page 72](#)
- [View Device Ports, on page 82](#)
- [View Device Interfaces, on page 82](#)
- [View Device Modules, on page 86](#)
- [View Environment Information \(Power Supplies, Fans\), on page 86](#)
- [View Device Neighbors, on page 87](#)
- [Get More Information About Links, on page 87](#)
- [View Circuits/VCs, on page 88](#)
- [View Satellites, on page 88](#)
- [Create User Defined Fields for Custom Values, on page 88](#)

## Find Devices

The quickest way to find a device is to use the quick search text boxes displayed at the top of the Network Devices table (**Inventory > Device Management > Network Devices**). You can enter partial strings for a device name, IP address, or software version, or choose from the values for reachability, admin status, and Inventory Collection. If user defined fields have been created, you can also search by user defined field values. Devices are also organized into device groups, which you can view by choosing **Inventory > Device Management > Network Devices** and selecting a device type from the **Device Group** list.

## Get Basic Device Information: Device 360 View

The Device 360 view is a pop-up window that provides quick information about a device, its inventory, and its status. This includes device alarms, modules, interfaces, neighbors, and chassis.

To launch a Device 360 view:

- Click the "i" icon next to an IP address in almost any device table
- From the network topology, click a device in an expanded group, then click **View**

The Device 360 view provides general device and performance information at the top of the view, and more detailed interface information in tabs in the lower part of the view. The information the Device 360 view displays depends on the device type and configuration. The Device 360 view provides the following information.

Information Provided in Device 360 View	Description
-----------------------------------------	-------------

General information and tools	<p>Device type, its OS type and version, its last configuration change, and its last inventory collection. Icons convey the status of the device.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• If you have opened the Device 360 view for a Cisco NCS 6000 device that houses a Secure Domain Router (SDR), the SDR's name is also listed.</li> <li>• If you have opened the Device 360 view for a Cisco Catalyst 6500 Series device with dual and quad-supervisor Virtual Switching System (VSS), the device's redundancy state, switch mode, and operational redundancy mode is also listed.</li> </ul> <p>Using the menus in the top right of the popup window, you can also perform these tasks:</p> <ul style="list-style-type: none"> <li>• Troubleshoot—Perform a ping or traceroute, launch the Alarm browser, open a Cisco support case, or get information from the Cisco Support Community (<b>Actions</b> menu)</li> <li>• Performance—Check device CPU and memory (<b>View &gt; Performance Graphs</b>)</li> <li>• Topology—View the network topology and the device's local topology, up to 3 hops (<b>Actions</b> menu)</li> <li>• Check the device's routing table (<b>Actions</b> menu)</li> <li>• Open the <b>Device Console</b> to enter commands you want to run on the device (<b>Actions</b> menu)</li> <li>• View the configuration that is currently running on the device (<b>Actions &gt; Show Command</b>)</li> <li>• Collect the device's inventory and save it to the database using <b>Sync Now</b> (<b>Actions</b> menu)</li> <li>• Open an HTTP, HTTPS, SSH, or Telnet session with the device (<b>Actions</b> menu)</li> <li>• Launch Cisco Transport Controller for optical devices (<b>Actions</b> menu)</li> <li>• Enable the automatic refresh of the view every 20 seconds (<b>Actions</b> menu)</li> <li>• Open the Device Details page to view details about software image and configuration file management, and use the device's Chassis View (by clicking the device IP address hyperlink or choosing <b>View &gt; Details</b>)</li> <li>• Select a device for a side-by-side comparison with another device on the basis of information such as raised alarms and the current status of circuits, interfaces, and modules (<b>Actions</b> menu)—see <a href="#">Compare Device Information and Status</a></li> </ul>
-------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Performance data	Charts reflecting various aspects of the device performance. If a device has multiple memory pools, the Device 360 view will display the average utilization for all of the memory pools. If you want to see information about individual memory pools, use the memory utilization dashlets in the Network Summary dashboard. See <a href="#">Network Summary Dashboard Overview</a> .
Alarms tab	Current alarms for the device, including their severity, status, and the time they were generated. Depending on the alarm source, you can also launch other 360 views from this tab.
Modules tab	Modules that are configured on the device, including their name, type, state, ports, and location.
Interfaces tab	Interfaces that are configured on the device, including status information. You can also launch an Interface 360 view for a specific interface.
Neighbors tab	NEs that are connected to this device through CDP (Cisco Discovery Protocol). If the selected device does not support CDP, this tab is empty. Displayed information includes device type and name, and the local port and device port. To view the neighbors in a popup topology map, choose <b>Actions &gt; N Hop Topology</b> from the top right of the Device 360 view (see <a href="#">View a Device's Local Topology from the Device 360 View, on page 67</a> ).
Circuit/VCs tab	Circuit/VC name, type, customer, status, and creation date for each circuit provisioned on the device. You can also launch a Circuit/VC 360 view for specific circuits/VCs.
Satellites tab	For Cisco ASR 9000 devices in a cluster configuration, lists a satellite's name, type, description, status, and IP and MAC addresses. You can also launch a Satellite 360 view for a specific satellite.
Civic Location	Geographical information about device's location.
Recent Changes	The last five changes made on the device, classified as: Inventory, Config (Configuration Archive), or SWIM (Software Images). (These are the same types of changes that are displayed when you choose <b>Inventory &gt; Network Audit</b> .)
SRRGs	Lists the Shared Risk Resource Groups (SRRGs) assigned to the device. Click this tab's ? ( <b>help</b> ) icon to view its legend. For more information about SRRGs, see <a href="#">View and Manage Shared Risk Resource Groups (SRRG) in the Geo Map</a> .

You can also view a specific device in the topology map by choosing **Actions > Network Topology** (at the top right of the Device 360 view).

## Compare Device Information and Status

From the **Comparison View**, you can perform a side-by-side comparison of multiple devices, viewing information such as raised alarms, the status of modules, interfaces, and circuits on those devices, and a summary of recent changes that have been made. To compare devices, do the following:



- 
- Step 1** Choose one of the following to open the **Network Devices** page:
- **Monitor > Managed Elements > Network Devices**
  - **Inventory > Device Management > Network Devices**
- Step 2** For each device you want to compare:
- a) Open its **Device 360** view by clicking the *i* (**information**) icon in the **IP Address** column.
  - b) Choose **Actions > Add to Compare**.
- The device you selected is displayed at the bottom of the page. You can select a maximum of 4 devices.
- Step 3** Click **Compare**.
- The **Comparison View** opens.
- Step 4** From the drop-down list at the top of the view, specify whether the view will show all available information or just the information that is unique to each device.
- Step 5** Click **Comparison View**, check the check box for the categories you want the view to display, and then click **Save**.
- By default, all of the categories are already selected.
- Step 6** Scroll down the page to view the information provided for each category you selected.
- Note the following:
- The **Comparison View** only displays information for two devices at a time. If you selected more than two, you will need to toggle to the devices that are not currently displayed.
  - To reorder the devices you have selected, click **Rearrange**.
  - Each device's **View** and **Actions** menu is identical to the ones provided in their **Device 360** view. If you select an option, the corresponding page opens.
  - You can minimize and maximize the categories displayed, as needed.
  - The **Comparison View** is also available for circuits and VCs, interfaces, and links. Whenever you select any of these elements from their respective 360 view for comparison, they are displayed in the corresponding tab. This allows you to switch between element types, as needed.
  - When you are done comparing devices, click **Back** at the top of the view and then click **Clear All** at bottom of the page. If tabs for other element types are still displayed, you will need to clear them as well.
- 

## View a Device's Local Topology from the Device 360 View

You can launch a small topology window from the Device 360 view that displays the network topology around a device, up to 3 hops.

- 
- Step 1** Open the Device 360 View for the device in which you are interested.

- Click the "i" icon next to an IP address in almost any device table.
- From the network topology, click a device in an expanded group, then click **View**.

**Step 2** Choose **N-Hop Topology** from the Actions drop-down menu (at the top right of the Device 360 view).

**Step 3** Adjust the popup window to show the information you need.

- Click the edit icon
- Select a hop count (1-3) from the Hop drop-down list.
- Select a topology map layout from the Layout drop-down list.

**Step 4** Save your changes, and use the pan and zoom tools to view the results.

---

## View the Network's Hardware Inventory

Use this procedure to view basic hardware information for all devices in the network—the product name, physical location, serial number, manufacture date, and so forth.

---

**Step 1** To view device-level information:

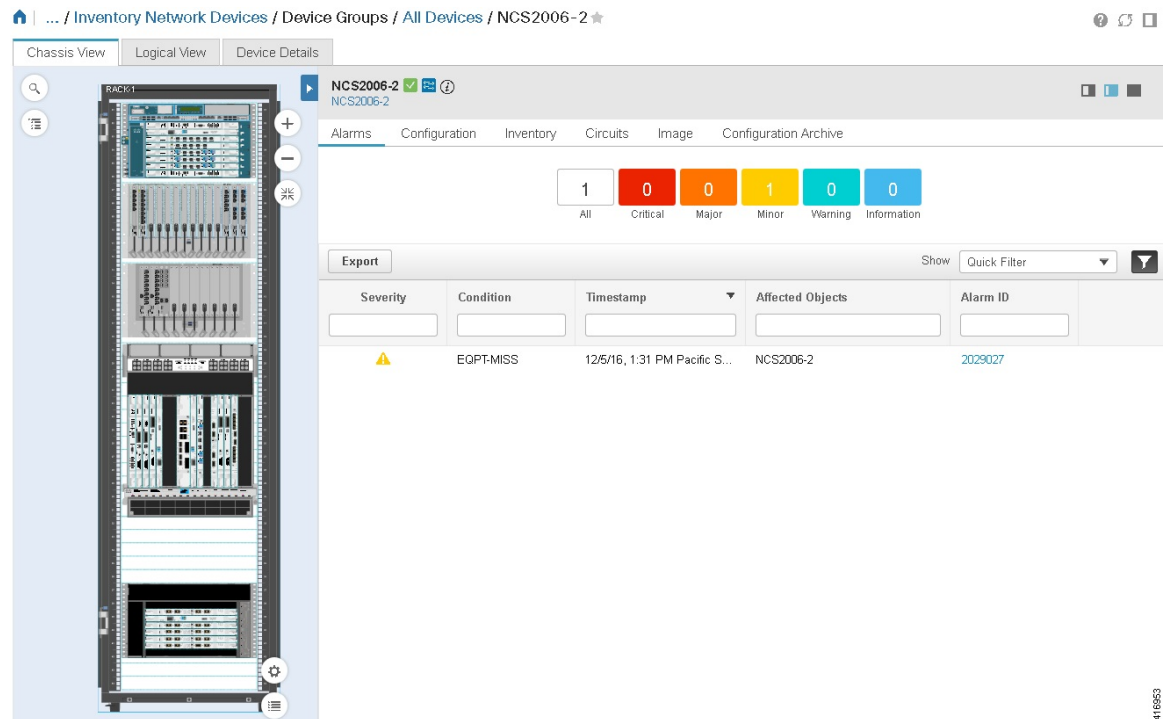
1. Choose **Inventory > Device Management > Network Inventory**.
2. Use the Quick Filters to locate specific devices. For example, to list the hardware information for all ASR devices, enter **\*ASR\*** in the Product Name field.

**Step 2** To view element-level information, use one of these methods:

- Get the information from the Device Details page. See [Get Complete Device Information: Device Details Page, on page 68](#).
  - Get the information from the Chassis View. See [Open the Chassis View, on page 72](#).
  - Run a hardware report. See [Device Reports, on page 259](#).
- 

## Get Complete Device Information: Device Details Page

For the most comprehensive information about a device, view the Device Details page. It provides in-depth inventory information and configuration options.



To launch the Device Details Page:

- From a Device 360 view—Click the IP address hyperlink or choose **View > Details**.
- From a network devices table—Click the device name hyperlink in a device table.

The tabs that are displayed here depend on your selection in the Chassis View. They are described in the following table:

Tab Name	Description
Chassis View	Provides inventory, service, and alarm information that is contextualized to the element you select. Also serves as launch point for configuration, Image management, and Configuration Archive features. (To configure logical elements, click the <b>Logical View</b> tab.)  For information on using the Chassis View features, see <a href="#">Overview of the Chassis View Window, on page 73</a> .
Logical View	Provides logical inventory information. Also provides configuration options for logical elements.
Device Details	Provides system information (environment, modules ports, interfaces, and other settings). The Summary page contains graphs indicating the average utilization of all CPUs and the average utilization of all memory components for the device.
Alarms	Get information about the alarms that have been raised on a device, a card, or a port. See <a href="#">View an Alarm's Details</a> .
Configuration	Configure a device, card, or port. Elements are grouped by their physical location. (To configure elements that are grouped according to their logical function, click the <b>Logical View</b> tab.) See <a href="#">Ways to Configure Devices Using Cisco Evolved Programmable Network Manager</a> .

Tab Name	Description
Inventory	View detailed hardware information such as serial numbers and manufacture dates for a device or card.
Interfaces	View the status of interfaces configured on a device, card, or port. From here, you can also open the <b>Interface 360</b> view for a particular interface. For links to topics that describe other ways to view interface information in Cisco EPN Manager, see <a href="#">View Device Interfaces</a> .
Performance	<p>View summary information and high-level performance metrics. Note the following:</p> <ul style="list-style-type: none"> <li>• If you are viewing the chassis view for any device other than a Cisco Converged Broadband Router-8 (cBR-8) router, information is displayed for the selected interface on a card or port. The dashlets displayed in addition to the <b>Interface Details</b> dashlet will vary, depending on the interface type you chose. After choosing an interface from the <b>Interface</b> drop-down list, make sure to click <b>Apply</b> in order to refresh the information that is displayed.</li> <li>• If you are viewing the chassis view for a Cisco cBR-8 router, information is also displayed for the device as a whole. You can view dashlets that provide information such as the number of voice calls that have been made and upstream/downstream utilization percentages. To ensure that information is collected and reported for the Cisco cBR-8 routers in your network, verify that <b>Cable Policies</b> is listed on the <b>Monitoring Policies</b> page (<b>Monitor &gt; Monitoring Tools &gt; Monitoring Policies &gt; Policies pane</b>), is currently active, and has polling intervals set for its parameters.</li> </ul> <p><b>Note</b> You can display up to 10 dashlets at a given point of time on the Performance tab. To choose these dashlets, click the Settings icon on the top right corner of the pane and use the <b>Add Dashlet(s)</b> option to make your selection.</p>
Circuits	View the circuits a device, card, or port participates in. For links to topics that describe other ways to view circuit information in Cisco EPN Manager, see <a href="#">View Circuits/VCS</a> .
Image	<p>Manage the software image that is running on the device. See <a href="#">View the Images That Are Saved in the Image Repository</a>.</p> <p><b>Note</b> This tab is only available when a top-level chassis is selected.</p>
Configuration Archive	<p>Manage the device configuration file that is running on the device. See <a href="#">View All Archived Files</a>.</p> <p><b>Note</b> This tab is only available when a top-level chassis is selected.</p>

## Configure Interfaces from the Device Details Page

Complete the following procedure to configure an interface from the Device Details page:

- 
- Step 1** With a device's Chassis View open, click the **Launch Configuration** link.  
The Device Details page opens.
- Step 2** Click the **Logical View** tab.

- Step 3** From the **Features** pane, choose **Interfaces** > the interface type you want to configure.
- Step 4** Complete the instructions specific to the interface type you chose to add or edit an interface (see [Configure Interfaces](#)).
- 

## Update Cisco NCS 1000 Interface Settings

You can quickly update the **Admin Status**, **Wavelength (nm)**, and **Loopback** settings for interfaces configured on a Cisco NCS 1000 Series device from its Device Details page. To do so, complete the following procedure.

---

- Step 1** Open the Device Details page for a Cisco NCS 1000 Series device, as described in [Get Complete Device Information: Device Details Page, on page 68](#).
- Step 2** Click the **Configuration** tab.
- The page updates, displaying 3 sub-tabs: **Optics**, **Ethernet**, and **Coherent DSP**.
- Step 3** Click the sub-tab for the interface type you want to update.
- Step 4** Make the necessary changes:

### Method 1

1. In the interfaces table, locate the interface you want to update.
2. Click the parameter you want to change to open a drop-down list.
3. Choose the value you want to set, then click **Save**.

### Method 2

1. Click the radio button for the interface you want to update, then click the pencil (**Edit**) icon.  
The **Edit interface type** dialog box opens.
2. Choose the value you want to set from the available drop-down lists, then click **Apply**.
3. Click **OK** to confirm your changes.

Note the following:

- For Optics interfaces:
  - You can update the **Admin Status** and **Wavelength (nm)** parameters.
  - You can only set a new wavelength value if the **Optics Type** parameter is set to **DWDM**.
- For Coherent DSP and Ethernet interfaces:
  - You can update the **Admin Status** and **Loopback** parameters.
  - You can only set a new loopback value if the **Admin Status** parameter is set to **Testing**.
  - If you set the **Loopback** parameter to **Line**, Cisco EPN Manager applies the same configuration applied for a facility loopback. A facility loopback tests the line interface unit (LIU) of a card, the electrical interface assembly (EIA), and related cabling.

- If you set the **Loopback** parameter to **Internal**, Cisco EPN Manager applies the same configuration applied for a terminal loopback.

## View and Manage Devices Using the Chassis View

The Chassis View provides an interactive model of a device chassis and its hardware elements. From the Chassis View you can:

- View the contents of a chassis.
- Check the state of chassis elements and quickly locate problems.
- View alarmed elements and launch views that provide alarm details.
- Configure interfaces (using the launch point that opens the Device Details page).


The elements that are displayed in the Chassis View depend on the device type and the elements that are configured on the device.

Note that Admin users do *not* have read/write access to chassis views by default. To enable access for this user group, open the **Users, Roles & AAA** page, choose **User Groups**, and then check the **Chassis View Read and Write** check box (under **Network Monitoring** in the **Tasks Permissions** tab). See [View and Change the Tasks a Group Can Perform](#).

See these topics for information about how to launch and use the Chassis View:

## Open the Chassis View

The following table describes the various ways you can open the Chassis View. If a device does not provide these launch points, it means the device does not support the Chassis View. For a list of devices that support the Chassis View, see [Device Support for the Chassis View in this release of Cisco EPN Manager](#), on page 76.

To open a Chassis View from:	Do the following:	The Chassis View is displayed in:
Network Devices table	Click  next to the device IP address.	A pop-up window
	Click a device name hyperlink.	A full-page view
Device 360 view	Choose <b>View</b> > <b>Chassis View</b> from the top right of the <b>Device 360</b> view.	A pop-up window
	Choose <b>View</b> > <b>Details</b> from the top right of the <b>Device 360</b> view.	A full-page view
Device Details page	Click the <b>Chassis View</b> tab.	A full-page view

To open a full-page Chassis View from a Chassis View pop-up window, click the **Launch Configuration** link in the top right corner of the window.

## Permissions Required to View and Configure Devices Using the Chassis View

The following table describes the Chassis View permissions that are granted to members of the Cisco EPN Manager user groups. These permissions cannot be edited. For more information on user groups, see [Control the Tasks Users Can Perform \(User Groups\)](#), on page 672

- Full access (read and write)—Users in this group can view and configure devices using the Chassis View.
- Read-only access—Users in this group can use the Chassis View to view devices but not to configure them.
- Write-only access—Users in this group can use the Chassis View to configure devices but not view them (only applies to the NBI Write group).
- No access—Users in this group cannot access or use the Chassis View.

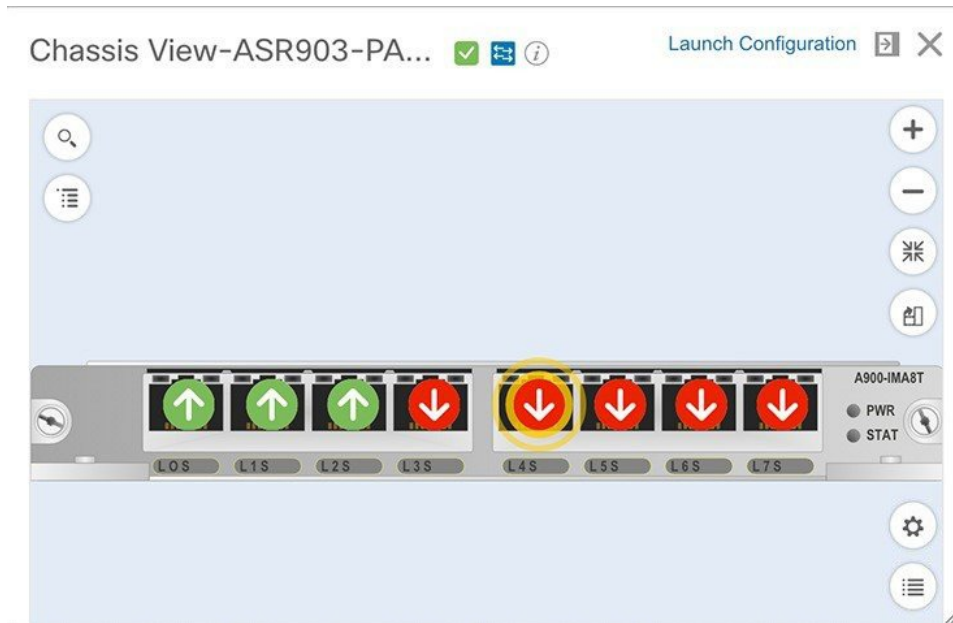
Group Type		Read	Write
Web UI	Root	X	X
	Super Users	X	X
	Admin	—	—
	Config Managers	X	X
	System Monitoring	X	—
	User-Defined 1-4	X	—
	Monitor Lite	X	—
NBI	NBI Credential	—	—
	NBI Read	X	—
	NBI Write	—	X
	North Bound API	X	X

## Overview of the Chassis View Window


The following illustration shows the Chassis View for a Cisco ASR 903 router.



In this example, the user then clicked a port that is currently down.



The Chassis View updates, displaying only the line card module that the port resides on and zooming in on it. The port pulsates in the Chassis View to help the user locate it. The badges displayed on the ports in this module indicate the primary status of those port (see [Port or Interface States, on page 78](#)). Some elements may be surrounded by colored lines to indicate their state (out of service, pre-provisioned, and so forth). To

open a key that explains the meaning of the badges and these other indicators, click  at the bottom right of the Chassis View.

















If a device has multiple chassis or shelves, each chassis or shelf is displayed in the same Chassis View (for an example, see [View Mixed Chassis, Multi-Chassis, and Multi-Shelf Devices in the Chassis View, on page 79](#)). If a card image cannot be retrieved, the Chassis View displays a question mark alongside the card name.

Note the following:

- The colors rendered in the Chassis View may not match your physical device because the Chassis View displays a generic image that is packaged with Cisco EPN Manager .
- If you have opened the Chassis View for a Cisco NCS 6000 device that houses a Secure Domain Router (SDR), both the device type and the SDR's name are displayed at the top of the Chassis View. Keep in mind that there may be cases where the SDR label for a device that belongs to a cluster or a user-defined group is not displayed (since auto-clustering is applied to devices based on their proximity).

The following table describes the Chassis View's components and their function:

Chassis View Component	Description
	Opens a field you can use to search for a particular rack, shelf, module, or interface on a device.
	Opens the <b>Chassis Explorer</b> .
	Indicates the device's reachability state (see <a href="#">Device Reachability and Admin States, on page 52</a> ). This example indicates the device is reachable.
	Indicates the device's administrative status (see <a href="#">Device Reachability and Admin States, on page 52</a> ). This example indicates the device is managed.
	Opens the device's <b>Device 360</b> view. See <a href="#">Get Basic Device Information: Device 360 View</a> .
Launch Configuration link	Opens the device's Device Details page. The tabs displayed on this page will vary, depending on whether a device, module, or port is currently selected in the Chassis View. See <a href="#">Get Complete Device Information: Device Details Page</a> .
	Adds a shortcut to the device's Chassis View in the <b>Dock</b> window. See <a href="#">Customize the Dock Window</a> .
	Closes the <b>Chassis View</b> .
	Zooms in on an image.
	Zooms out from an image.
	Resizes an image so it can be viewed in its entirety within the <b>Chassis View</b> .
	Opens a pop-up window that allows you to .

Chassis View Component	Description
	<p>Toggles between the front and rear Chassis View for a device that supports this feature. A callout that appears when you place your cursor over this icon indicates which view you are opening.</p> <p>This feature is supported by the following Cisco devices:</p> <ul style="list-style-type: none"> <li>• ASR 901S</li> <li>• cBR-8</li> <li>• NCS 1001, 1002, 5001, 5002, and 5008</li> </ul>
	Rotates the image of the module that is currently displayed. This icon is not available when an entire device is displayed.
	Click to access the <b>Enable Alarm Blinking</b> check box. When checked, any alarm badges displayed for a module or port will blink in order to draw attention to them and make them easier to locate.
	Opens a key that explains the significance of badges and colored lines displayed in the <b>Chassis View</b> .

## Device Support for the Chassis View in this release of Cisco EPN Manager

The following table lists the Chassis View features and the devices on which they are supported. This means the feature has been tested and verified on that device. While you can launch the Chassis View from other devices, it has only been verified on the devices below.

Feature	Supported Devices:
---------	--------------------

General features	Cisco NCS 1001 Cisco NCS 1002 Cisco NCS 2000 Cisco NCS 4000 and 4200 Cisco NCS 5001 Cisco NCS 5002 Cisco NCS 5011 Cisco NCS 5501 and 5501-SE Cisco NCS 5502 and 5502-SE Cisco NCS 6008 Cisco ONS Cisco Catalyst 6504-E Cisco ASR 900 Cisco ASR 9000 Cisco cBR-8
Multi-chassis information	Cisco NCS 2000 Cisco ONS Cisco ASR 9000
Operational States	Cisco NCS 1002 Cisco NCS 2000 Cisco NCS 4000 and 4200 Cisco ONS Cisco ASR 900 Cisco ASR 9000 Cisco cBR-8
Alarms	Cisco NCS 1002 —Port, card, module, equipment alarms Cisco NCS 2000 —Port, card, module, equipment alarms Cisco NCS 4000 and 4200 —Port alarms Cisco ONS Cisco ASR 900 —Port, card, module, equipment alarms Cisco ASR 9000 —Port, card, module, equipment alarms Cisco cBR-8 device

## View Network Element State Information in the Chassis View

Badges, lines, and colors provide information about the operational state, elements and components in a device. Click the **Legends** icon at the bottom right of the Chassis View to display a key that lists what the badges, lines and colors mean.

See these topics for more information:

- [Equipment Operational States \(Chassis View\)](#), on page 78
- [Port or Interface States](#), on page 78






### Note

Port state information is not shown for the CFP ports on an A9K-400G-DWDM-TR line card as these ports are not yet supported.




## Equipment Operational States (Chassis View)

The equipment operational states represent the running state of the network element.

Equipment Operational State	Icon	Description
In Service	(none)	Equipment is operating properly.
Pre-provisioned		(Cisco NCS 2000 and Cisco ONS devices only) Equipment has been configured but is not physical present in the chassis.
Failed/Disabled/Down/Out of Service/Out of Service Maintenance		Equipment is not operating properly.
Unknown		Equipment operational state is unknown. No response (or insufficient response) from the device.

## Port or Interface States

**Port or Interface Primary States**—Conveys the most important state information for a port or interface by combining the admin and operational states. The Multilayer Trace displays either a port's primary state or alarm status. For the Chassis View, if an element does not support the changing of color to indicate a state change, you can still get the state change information from the alarm that is generated.

Port or Interface Primary State	Icon	Admin Status	Operational State
Unknown		Unknown	Unknown
Down		Up	Down
Test		Test	—

Admin Down		Admin Down	—
Up		Up	Up
Auto Up		Up	Auto Up

**Port or Interface Admin Status**—Represents the configured state of the port or interface (for example, if an administrator has manually shut down a port).

Port or Interface Admin Status	Icon	Description
Unknown		Port or interface admin status is unknown. There is no response (or insufficient response) from the device.
Admin Down		Port or interface was manually shut down by the administrator.
Up		Port or interface is enabled by the administrator.
Test		Port or interface is being tested by the administrator.

**Port or Interface Operational State**—Conveys the port or interface's running state and whether it is working properly.

Port or Interface Operational State	Icon	Description
Unknown		Port or interface operational state is unknown. There is no response (or insufficient response) from the device.
Down		Port or interface is not working properly.
Up		Port or interface is receiving and transmitting data.
Auto Up		Port or interface is receiving and transmitting data (only certain devices support this state; other devices use "Up").

## View Mixed Chassis, Multi-Chassis, and Multi-Shelf Devices in the Chassis View

The following example shows a mixed Chassis View that has both Cisco NCS 2000 and Cisco ONS 15454 chassis. Shelf numbers are not consecutive because of the different types of chassis.

## View Alarms in the Chassis View

The screenshot shows the Cisco EPN Manager interface. The top navigation bar includes 'Inventory Network Devices / Device Groups / All Devices / NCS2KE'. The main view is 'Chassis View' for device 'NCS2KE'. On the left, a physical rack diagram shows two racks, RACK1 and RACK2, with various modules installed. On the right, a table lists the inventory items:

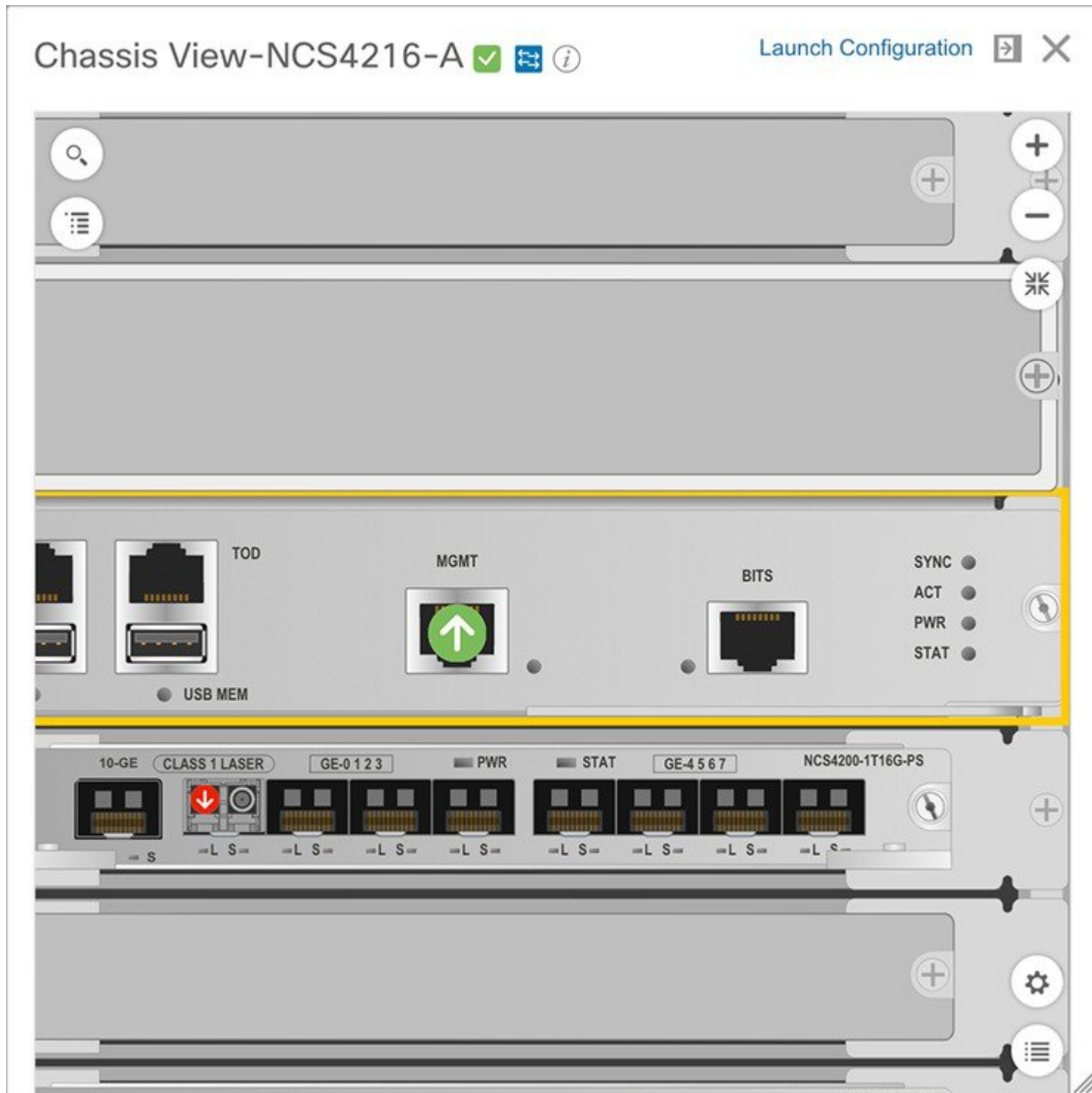
Location	Product ID	Oper...	Product N...	Type	Seri...	CLEL...
▼ 0				RACK		
RACK-1[39-1]		Enabled		Module		
RACK-1[39-1]		Enabled		Module		
RACK-1[37-1]		Enabled		Module		
▼ RACK-1[07]	15454-M6-SA	Enabled	NC	Chassis		
▶ SHELF-1	15454-M-TNC-I-9	Enabled	TNC	Module	CAT16...	WOCU...
SHELF-1		Disabled		Module		
SHELF-1	15454-M6-DC	Unknown	M6-DC	Module	SAL16...	WOPU...
SHELF-1	15454-M6-SA	Unknown	M6-SA	Module	SAL16...	WOM...
SHELF-1	15454-M6-ECU	Unknown	M6-ECU	Module	SAL16...	WOM...
SHELF-1	15454-M6-FTA	Unknown	M6-FTA	Module	SAL16...	WOCU...
SHELF-1	15454-M6-LCD	Unknown	M6-LCD	Module	SAL16...	WOP...
▶ SHELF-1		Disabled		Module		
SHELF-1		Disabled		Module		
▶ SHELF-1		Disabled		Module		
SHELF-1		Disabled		Module		
SHELF-1		Disabled		Module		


For mixed-chassis, multi-chassis, and multi-shelf devices, Cisco EPN Manager aggregates alarms to a chassis or shelf as explained in [View Alarms in the Chassis View, on page 80](#).

For multi-chassis devices in a cluster, the Device 360 view's **Chassis** tab identifies which chassis is the primary and which is the backup.


## View Alarms in the Chassis View

An alarm badge in the Chassis View represents one or more alarms that have been localized to a piece of equipment. For an element with multiple alarms, the badge icon will convey the most severe alarm.



To customize the Chassis View so that alarm icons blink (to bring your attention them), click  from the bottom right of the view, then check the **Enable Alarm Blinking** check box.

To view the alarms specific to a device, do the following:

- 
- Step 1** With a device's Chassis View open, click the **Launch Configuration** link.  
The Device Details page opens.
- Step 2** If not already selected, click the **Alarms** tab.  
All of the alarms that have been raised for the device are listed here.
- Step 3** To view the alarms for a specific device component (such as a line card or port), do one of the following:
- Double-click the component in the Chassis View.
  - Click  to open the **Chassis Explorer**, then click its entry.
- 

## View Device Ports

You can get in-depth information about a device's physical ports from the Device Details page. You can also get basic port information from various 360 views.

To view a device chassis with its modules and ports, use the Chassis View. See [Open the Chassis View, on page 72](#).

To view this port information:	Do the following:
All Physical ports on a device (including port alias and residing module)	<ol style="list-style-type: none"> <li>1. Open the Device Details page. <ul style="list-style-type: none"> <li>• Choose <b>View &gt; Details</b> from the top right of the Device 360 view.</li> <li>• Click the device name hyperlink in a device table.</li> </ul> </li> <li>2. Under the <b>Device Details</b> tab, choose <b>System &gt; Physical Ports</b>.</li> </ol>
An interface's ports	Check the <b>Interface</b> tab on a 360 view
Ports connected to a module	Check the <b>Modules</b> tab on a Device 360 view
Ports connected to a neighbor	Check the <b>Neighbors</b> tab on a Device 360 view

For a matrix of ports states and icons, see [Port or Interface States, on page 78](#).

## View Device Interfaces

Cisco EPN Manager provides the following ways to view device interfaces:

Ways to View Interfaces	For more information, see:
-------------------------	----------------------------



View details about a specific interface	<a href="#">Get a Quick Look at a Device Interface: Interface 360 View, on page 83</a>
View a specific device's interfaces	<ul style="list-style-type: none"><li>• <a href="#">View a Specific Device's Interfaces: Device 360 View, on page 83</a></li><li>• <a href="#">Get Comprehensive Information About a Device's Interfaces Using the Device Details Page, on page 85</a></li></ul>

## View a Specific Device's Interfaces: Device 360 View

Use the Device 360 view to quickly check the status of a device's interfaces.

### Step 1

Open the Device 360 view:

- Click the "i" icon next to an IP address in almost any device table
- From the network topology, click a device in an expanded group, then click **View**

### Step 2

Click the **Interfaces** tab.

## Get a Quick Look at a Device Interface: Interface 360 View

The Interface 360 view gives you a quick summary about a specified interface. In addition to status, performance, and general interface information, you can enable and disable the interface from the Interface 360 view. The Interfaces 360 view also provides ways to open 360 views for circuits/VCs (depending on the interface configuration).

You can launch the Interface 360 view wherever you see an "i" icon next to an interface name—for example, in an alarms table, or in the various 360 views under the Interfaces or Endpoints tabs.

You can also view a specific interface in the topology map by choosing **Actions > Show in Topology** (at the top right of the Interface 360 view).

The Interface 360 view provides general interface and performance information at the top of the view, and more detailed interface information in tabs in the lower part of the view. The information the Interface 360 view displays depends on the interface configuration.



#### Note

The tabs displayed will vary, depending on the type of interface for which you launched this view.

Information Provided in Interface 360 View	Description
--------------------------------------------	-------------

General information	<p>The interface name, status, description, type, device name; IP address, MAC address, and so forth. Using the menus in the top right of the pop-up window, you can also perform these tasks:</p> <ul style="list-style-type: none"> <li>• Open a chassis view that highlights the port or line card the interface is associated with (<b>View</b> menu). This feature comes in handy when you need to describe to an onsite technician where to find the source of an issue.</li> <li>• Select the interface for a side-by-side comparison with another interface on the basis of information such as raised alarms and the current status of associated circuits and VCs (<b>Actions</b> menu)—see <a href="#">Compare Interface Information and Status</a>.</li> <li>• View performance information for optical devices by opening the <b>DWDM/OTN Performance</b> dashboard from the <b>View</b> menu. See <a href="#">DWDM/OTN Performance Dashboard Overview</a>.</li> <li>• Enable and disable the interface from the <b>Actions</b> menu.</li> <li>• Enable and disable the lockout of an MPLS interface from the <b>Actions</b> menu. You would lock out an MPLS interface before doing maintenance work on the TE Tunnel link that the interface belongs to. After you lock out an MPLS interface, be sure to manually sync the device. Otherwise, you will not have the option to disable the lockout later.</li> <li>• View the device on which the interface is located in a topology map (<b>Actions</b> menu).</li> </ul>
Performance data	Graphs or charts reflecting various aspects of interface performance.
Alarms	Current alarms for the interface, including their severity, status, and the time they were generated. Also provides a launch point to the Alarm Browser.
Interfaces	Name, interface type, and operational and admin status for each associated interface. Also provides a launch point for the Interface 360 view.
Circuit/VCs	(For interfaces that participate in circuits) Circuit/VC name, type, customer, status, and creation date. Also provides a launch point for the Circuit/VC 360 view.
EFPs	All EFPs associated with the interface. Also provides their operational status, admin status, and EFP type.
Optical Physical	Real-time performance monitoring data for the interface. This data is collected every 10 seconds, and the results of the last 10 pollings are displayed here. For a listing of the counters that can be displayed, see <a href="#">Performance Counters for Optical Monitoring Policies</a> .

## Compare Interface Information and Status

From the **Comparison View**, you can perform a side-by-side comparison of multiple interfaces, viewing information such as IP and MAC address, raised alarms, and associated circuits and VCs. To compare interfaces, do the following:

- 
- Step 1** For each interface you want to compare:
- Open its **Interface 360** view, as described in [Get a Quick Look at a Device Interface: Interface 360 View](#).
  - Choose **Actions > Add to Compare**.
- The interface you selected is displayed at the bottom of the page. You can select a maximum of 4 interfaces.
- Step 2** Click **Compare**.
- The **Comparison View** opens.
- Step 3** From the drop-down list at the top of the view, specify whether the view will show all available information or just the information that is unique to each device.
- Step 4** Click **Comparison View**, check the check box for the categories you want the view to display, and then click **Save**.
- By default, all of the categories are already selected.
- Step 5** Scroll down the page to view the information provided for each category you selected.
- Note the following:
- The **Comparison View** only displays information for two interfaces at a time. If you selected more than two, you will need to toggle to the interfaces that are not currently displayed.
  - To reorder the interfaces you have selected, click **Rearrange**.
  - Each interface's **View** and **Actions** menu is identical to the ones provided in its **Interface 360** view. If you select an option, the corresponding page opens.
  - You can minimize and maximize the categories displayed, as needed.
  - The **Comparison View** is also available for circuits and VCs, devices, and links. Whenever you select any of these elements from their respective 360 view for comparison, they are displayed in the corresponding tab. This allows you to switch between element types, as needed.
  - When you are done comparing interfaces, click **Back** at the top of the view and then click **Clear All Items** at bottom of the page. If tabs for other element types are still displayed, you will need to clear them as well.
- 

## Get Comprehensive Information About a Device's Interfaces Using the Device Details Page

Use the Device Details page to get extensive information about all of the interfaces that are configured on a device. For easier navigation, interfaces are grouped together by type.

- 
- Step 1** Open the Device Details page.
- Click the device name hyperlink which appears in many of the device tables
  - Choose **View > Details** at the top right of the Device 360 view

- Step 2** Under the Device Details tab, double-click **Interfaces** to display a list of all interfaces (of all types) that are configured on the device.
- Step 3** To display all interfaces of the same type, click the type (such as **Ethernet Interfaces**).
- Step 4** To get details about a specific interface, click the interface name hyperlink.

## View Device Modules

To view device module information, choose **Inventory > Device Management > Network Devices**, then launch a Device 360 or Device Details page, depending on how much information you want.

To get this information:	Use this navigation:
Basic module information: Status, type, ports	<p>From the Device 360 view, click the <b>Modules</b> tab. To open the Device 360 view:</p> <ul style="list-style-type: none"> <li>Click the “i” icon next to the device name in almost any device table</li> <li>From the Network Topology, click a device (in an expanded view), then click <b>View</b></li> </ul>
Module equipment type and power information	<p>From the Device Details page, choose <b>System &gt; Modules</b> under the Device Details tab.</p> <p>To open the Device Details page:</p> <ul style="list-style-type: none"> <li>Click the device name hyperlink which appears in many device tables</li> <li>Choose <b>View &gt; Details</b> from the top right of the Device 360 view</li> </ul> <p><b>Note</b> Due to a limitation in the retrieval of module related information, this page lists SFP transceivers of Cisco CAT6500 devices as 'Unspecified' products.</p>

## View Environment Information (Power Supplies, Fans)

Environment-related information, such as details about power supplies and fans, is displayed in a device's **Device Details** page. To access this information:

- Step 1** Do one of the following:
- Click the device name hyperlink that appears in many Cisco EPN Manager device tables and then click the **Device Details** tab (if it is not already selected).
  - Choose **View > Details** from the top right of a **Device 360** view and then click the **Device Details** tab (if it is not already selected).
- Step 2** From the **Features** pane, choose **System > Power Options & Fans**.

## View Device Neighbors

Device neighbor information, such as the neighbor name, port number, index, and duplex setting, is displayed in a device's **Device 360** view.

**Step 1** Open the **Device 360** view:

- Click the *i* (**information**) icon next to the device name in almost any device table
- From the network topology, click a device in an expanded group and click **View**

**Step 2** Click the **Neighbors** tab.

### Example

For example:

Name	Index	Port	Duplex
ASR9K	7	TenGigE0/0/2/0	fullduplex
CPE-ISR02	67	GigabitEthernet0/0/3	fullduplex
Asr_903	36	GigabitEthernet0/0/0	fullduplex

## Get More Information About Links

Cisco EPN Manager provides a variety of ways that you can view links and get more details about them:

To view link information for:	See the procedures in:
A specific link	<a href="#">Get a Quick Look at a Specific Link: Link 360 View, on page 160</a>
A specific link in a topology map	<a href="#">View a Specific Link in the Topology Map, on page 163</a>
A group in a topology map	<a href="#">View a Device Group's Links in a Network Topology Map, on page 163</a>
All of Cisco EPN Manager	<a href="#">View Link Tables , on page 164</a>

## View Circuits/VCs

Cisco EPN Manager provides a variety of ways that you can view circuits/VCs:

To view circuit/VC information for:	See the procedures in:
A specific circuit/VC in a topology map, in a Circuit/VC 360 view, or in a Circuit/VC Details page	<ul style="list-style-type: none"> <li>• <a href="#">Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 528</a></li> <li>• <a href="#">Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 532</a></li> </ul>
A device	<a href="#">View a Specific Device's Circuits/VCs, on page 534</a>
A device group in a topology map or in an expanded table	<a href="#">View a Device Group's Circuits/VCs, on page 535</a>
All of Cisco EPN Manager	<a href="#">View All Circuits/VCs in Cisco EPN Manager , on page 536</a>

## View Satellites

Cisco EPN Manager provides the following ways to view satellite information for host-satellite configurations:

Ways to View Satellites	For more information, see:
View all satellites in a location group using a topology map	<a href="#">View Cisco ASR 9000 Host-Satellite Topologies in the Topology Map, on page 235</a>
View a specific device's satellites from a Device 360 view	<ul style="list-style-type: none"> <li>• <a href="#">Identify the Satellites Connected to a Cisco ASR 9000 Host, on page 236</a></li> <li>• <a href="#">Get Basic Device Information: Device 360 View, on page 63</a></li> </ul>
View details about a specific satellite, including the hosts it is connected to, using the Satellite 360 view	<a href="#">Identify the Hosts Connected to a Satellite, on page 238</a>

## Create User Defined Fields for Custom Values

If you want to assign custom attributes to devices or circuits/VCs, you can create your own fields to be shown in the tables and you can define custom values in those fields. For example, you might want to label certain devices with a customer name. After you have created user defined fields and assigned values, you can search by these values in the device tables and in the maps.

To create user defined fields:

---

**Step 1** Choose **Administration > Settings > System Settings > Inventory > User Defined Fields**.

**Step 2** Click the '+' icon and create a new label and description.

**Step 3** Assign values in your newly created user defined field for specific devices/circuits/VCS as follows:

- a) Go to the device table or to the table of circuits/VCS.
  - b) Display your user defined field as a column in the table by clicking the settings icon at the top right of the page, choosing **Columns**, and then selecting your user defined field.
  - c) Go to the required device or circuit/VC in the table, enter a value in your user defined column, and click **Save**.
-







## CHAPTER 4

# Manage Device Configuration Files

---

- [Set Up Device Configuration File Management](#), on page 91
- [How Do I Find Out the Last Time Files Were Archived?](#), on page 95
- [Back Up Device Configuration Files to the Archive](#), on page 95
- [View the Device Configuration Files That Are Saved in the Archive](#), on page 97
- [View a Device's Running Configuration File \(Raw Content\)](#), on page 99
- [Label Important Configuration Files With Tags](#), on page 99
- [Synchronize Running and Startup Device Configurations](#), on page 99
- [Download Configuration Files](#), on page 100
- [Compare or Delete Device Configuration Files](#), on page 100
- [Deploy an External Configuration File to a Device](#), on page 101
- [Overwrite a Startup Configuration with a Running Configuration](#), on page 102
- [Roll Back a Device's Configuration To an Archived Version](#), on page 102
- [Export Configuration Files to a Local File System](#), on page 104
- [Delete Archived Device Configuration Files](#), on page 104
- [Check the Network Audit for Configuration Archive Operations](#), on page 105

## Set Up Device Configuration File Management

- [Make Sure Devices Are Configured Correctly](#), on page 91
- [Control How Archiving is Triggered](#), on page 92
- [Set Up Event-Triggered Archiving](#), on page 92
- [Specify Items to Be Excluded When Configuration Files Are Checked for Changes](#), on page 93
- [Control the Timeouts for Configuration Archive Operations](#), on page 93
- [Control How Often the Archive Summary Is Updated](#), on page 94
- [Control How Many Files Can Be Archived In Parallel](#), on page 94
- [Control Whether Configuration File Content Is Masked During Exports](#), on page 94
- [Control When Device Configuration Files are Purged from the Database](#), on page 94

## Make Sure Devices Are Configured Correctly

Before you start using the Configuration Archive features, make sure devices are configured according to the settings in [Configure Devices So They Can Be Modeled and Monitored](#), on page 34.

## Control How Archiving is Triggered

By default, Cisco EPN Manager saves device configuration files to the archive when:

- A new device is added to Cisco EPN Manager
- When a device change notification is received

Users with Administrator privileges can change those settings.

**Step 1** Choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive**.

**Step 2** Adjust the archiving settings depending on the following criteria.

Check this check box:	To archive files:
Archive configuration out-of-box?	When a new device is added (enabled by default)
Archive configuration after inventory sync?	When a change is detected after inventory collection (disabled by default)
Archive configuration on receiving configuration change events?	When a configuration change notification is sent (enabled by default); see <a href="#">Set Up Event-Triggered Archiving, on page 92</a>

**Step 3** To schedule regular archiving for groups of devices (or single devices):

- Choose **Inventory > Device Management > Configuration Archive**.
- Under the Devices tab, select the devices or device groups that you want to archive on a regular basis.
- Click **Schedule Archive** and complete the schedule settings in the **Recurrence** area. If the operation will be performed on a large number of devices, schedule the archiving for a time that is least likely to impact production.

**Note** To enable device configuration collection via SFTP, the configuration is copied to the 'localdisk/sftp' directory. By default, this option is disabled. To enable it, locate the 'ifm\_config\_archive.properties' file under the '/opt/CSColumos/conf/ifm' folder, and set the 'COPY\_CONFIGURATIONS\_TO\_LOCAL\_STORAGE' value to true. This is applicable only to the newly archived configuration files. Configuration files that were archived in the past are not copied to this directory.

## Set Up Event-Triggered Archiving

By default, Cisco EPN Manager backs up a device's configuration file whenever it receives a change notification event. This function will work only if devices are configured properly; see [How Is Inventory Collected?, on page 33](#). For example, for devices running Cisco IOS XR and Cisco IOS XE, the following setting must be configured:

```
logging server-IP
```

When Cisco EPN Manager receives a configuration change event, it waits 10 minutes (by default) before archiving in case more configuration change events are received. This prevents multiple collection processes from running at the same time. To check or change this setting, choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive** and adjust the Hold Off Timer.



**Note** The Hold Off Timer may be set to a shorter period for certain events, called expedited events. For more information, see [Change the Behavior of Expedited Events, on page 711](#).

To turn off event-triggered archiving, choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive** and uncheck the **Archive configuration on receiving configuration change events?** check box.

## Specify Items to Be Excluded When Configuration Files Are Checked for Changes

Some lines in device configuration files should be excluded when Cisco EPN Manager compares different versions to identify changes. Cisco EPN Manager excludes some lines by default, such as clock settings for routers and switches. If you have Administrator privileges, you can check which lines are excluded, and add more lines to be excluded.

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive**.
  - Step 2** Click the Advanced tab.
  - Step 3** In the Product Family list, choose the devices or groups to which you want to apply the command exclusions.
  - Step 4** In the Command Exclude List, enter a comma-separated list of configuration commands you want to exclude for that selection. These are the parameters Cisco EPN Manager will ignore when checking devices for configuration changes.
  - Step 5** Click Save.
- 

## Control the Timeouts for Configuration Archive Operations

By default, Configuration Archive operations such as archiving, rolling back, and fetching configurations from devices will time out if a device does not respond for 6 minutes (360s). To adjust this setting, choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive** and change the setting in the **Timeout** field.

## Control How Often Alarms are Triggered

By default, Cisco EPN Manager saves device configuration files to the archive based on the configured settings. However when these jobs fail, you can choose to generate an alarm notification.

When a Configuration Archive job fails, Cisco EPN Manager waits for 7 days or for more than 5 (by default) configuration files before triggering an alarm. The alarm has information about the cause for the trigger of the alarm and other related details associated with the configuration archives. To change the default settings for how often the alarms are generated, choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive** and adjust the Alarm Threshold parameter for maximum number of configuration files (exceeding which an alarm is generated) and the number of days to wait before the alarm is triggered.

## Control How Often the Archive Summary Is Updated

When you choose **Inventory > Device Management > Configuration Archive**, Cisco EPN Manager lists the configuration archives that it has collected. This summary data is updated whenever a new archive is collected. It is also updated by default at least every 30 minutes according to a summary refresh timer. You can change the time setting by choosing **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive** and adjust the **Summary refresh hold-off time**.

## Control How Many Files Can Be Archived In Parallel

Cisco EPN Manager uses 10 thread pools for copying configuration files to the archive. A larger number may be helpful when archiving of changes involving more than 1,000 devices; however, making the number too large can negatively impact system performance. To change this number, choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive** and adjust the **Thread Pool Count** value.

## Control Whether Configuration File Content Is Masked During Exports

Cisco EPN Manager supports exporting startup and running configuration files to a local file system. By default, the contents of these files are masked when they are exported. To export configuration files, see [Export Configuration Files to a Local File System, on page 104](#). If you want to change the mask setting, choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive** and adjust the **Mask security content while exporting** option.

## Control When Device Configuration Files are Purged from the Database

Device configuration files cannot be automatically deleted from the database (you can manually delete the files); they can be periodically purged by Cisco EPN Manager based on your settings. Users with Administrator privileges can adjust when configuration files are purged as follows. If you do not want any configuration files purged, follow this procedure but leave both fields blank.



### Note

For a description of how to manually delete a configuration file, see [Delete Archived Device Configuration Files](#).

**Step 1** Choose **Administration > Settings > System Settings**, then choose **Inventory > Configuration Archive**.

**Step 2** Adjust the archiving settings depending on the following criteria.

Use this field:	To purge files when:
Maximum ____ configuration archives	The number of a device's configuration files exceeds this setting (5 by default).
Maximum ____ days retained	A configuration file's age exceeds this setting (7 days by default).

# How Do I Find Out the Last Time Files Were Archived?

- 
- Step 1** To find out the most recent date when device running configuration files were backed up to the archive, choose **Inventory > Device Management > Configuration Archive** and click the **Devices** tab. The Latest Archive column lists the archiving time stamp for each device with the most recent archive listed first. The Created By column displays the archive trigger (for example, a syslog).
- Step 2** To view the contents of a device's most recently-archived running configuration file, click the time stamp hyperlink. The Running Configuration window displays the contents of the file.
- Step 3** To view the changes that were made between archives for a device, see [Compare or Delete Device Configuration Files, on page 100](#).
- 

## Back Up Device Configuration Files to the Archive

- [What Is Backed Up to the Database?, on page 95](#)
- [Back Up \(Archive\) Configuration Files, on page 96](#)

## What Is Backed Up to the Database?

The configuration archive maintains copies of device configuration files, storing them in the database. Most configuration files are stored in readable format as received from the device and can be compared with earlier versions. Device configurations can be restored to earlier states using the files saved in the archive.

If the running and startup configurations on a device are the same, Cisco EPN Manager copies only the running configuration to the database. This is why in some cases, when you view the image repository, you will only see an archive for the running configuration.

If a configuration file has not changed since its last backup, Cisco EPN Manager does not archive the file. Cisco EPN Manager will report that the job was successful and the job result will display **Already Exists**.

Cisco EPN Manager collects and archives the following device configuration files.

Device/Device OS	What is Backed Up
Cisco IOS and Cisco IOS XE	Latest startup, running, and VLAN configuration.
Cisco IOS XR	<ul style="list-style-type: none"> <li>• Latest running configuration; includes active packages. Devices must be managed with system user because copy command is not available in command-line interface (CLI) for non-system users.</li> <li>• Database configuration (binary file)</li> </ul> <p><b>Note</b> For Cisco NCS 4000 devices, the database is backed up as a .tgz file to a file system on your local machine.</p>

Device/Device OS	What is Backed Up
Cisco NCS	<p>Database configuration (binary file)</p> <p><b>Note</b> For Cisco NCS 2000 devices, the database is backed up as a binary file. Because it is not a text file, you cannot compare versions, but you can identify them by their file time stamp in the configuration archive.</p>

## Back Up (Archive) Configuration Files

When a configuration file is backed up, Cisco EPN Manager fetches a copy of the configuration file from the device and copies (backs it up) to the configuration archive (database). Before saving a copy to the archive, Cisco EPN Manager compares the fetched file with the last version in the archive (of the same type—running with running, startup with startup). Cisco EPN Manager archives the file only if the two files are different. If the number of archived versions exceeds the maximum (5, by default), the oldest archive is purged.

For devices that support both a running and startup configurations, Cisco EPN Manager identifies *out-of-sync* (unsynchronized) devices during the backup process by comparing the latest version of the startup configuration with the latest version of the running configuration file. For more information on out-of-sync devices, see [Synchronize Running and Startup Device Configurations, on page 99](#).

The following table describes the supported backup methods and how they are triggered. To check or adjust the default settings, see [Control How Archiving is Triggered, on page 92](#).

When you archive a Cisco NCS 2000 database, if you receive an error message saying the database or flash is busy, it is likely caused by one following:

- You are performing the archive operation in parallel with other Configuration Archive or Image Management operations. You should retry the operation after a short period of time.
- Multiple users are performing the same operation at the same time. You should retry the operation after a short period of time.
- The device has a software download alarm that has not been cleared. You should clear the alarm.



**Note** To enable device configuration collection via SFTP, the configuration is automatically copied to the 'localdisk/sftp' directory. This is applicable to only newly archived configuration files. Configuration files that were archived in the past are not copied to this directory. To disable this option, locate the 'ifm\_config\_archive.properties' file under the '/opt/CSColumos/conf/ifm' folder, and set the 'COPY\_CONFIGURATIONS\_TO\_LOCAL\_STORAGE' value to false.

**Table 7: Backup Method**

Backup Method	Description	Notes
On-demand manual backup	Choose <b>Inventory &gt; Configuration Archive</b> , choose devices, and click <b>Schedule Archive</b> (run the job immediately or at a later time).	N/A

Backup Method	Description	Notes
Regular scheduled backups	Choose <b>Inventory &gt; Configuration Archive</b> , choose devices, and click <b>Schedule Archive</b> . In the scheduler, specify a <b>Recurrence</b> .	N/A
Inventory collection backups	Cisco EPN Manager automatically performs backup if changes are detected during inventory collection.	Disabled by default
New device backups	Cisco EPN Manager automatically performs backup for new devices.	Enabled by default
Event-triggered backups (device change notifications)	Cisco EPN Manager automatically performs backup when it receives a syslog from a managed device.	Enabled by default

## View the Device Configuration Files That Are Saved in the Archive

- [View All Archived Files, on page 97](#)
- [View Archived Files for a Specific Device, on page 98](#)

### View All Archived Files

To view the configuration files that are saved in the database, choose **Inventory > Device Management > Configuration Archive**. Click the Archives or Devices tabs depending on where you want to start:

- **Archives** tab—A list of configuration files that have been archived, with the most recent archives listed first. The Out of Band column indicates whether the change was made by an application other than Cisco EPN Manager. Use the Groups list on the left to view archives by device types and families. From here you can:
  - [Roll Back a Device's Configuration To an Archived Version, on page 102](#)
  - [Overwrite a Startup Configuration with a Running Configuration, on page 102](#)
  - [Label Important Configuration Files With Tags, on page 99](#)
- **Devices** tab—A flat list of devices with their archived configurations. From here you can:
  - Schedule backups to the archive (see [Back Up Device Configuration Files to the Archive, on page 95](#)).
  - View the archived file for a specific device by clicking the device name hyperlink (see [View Archived Files for a Specific Device, on page 98](#)).

By default, Cisco EPN Manager saves up to 5 versions of a file, and deletes any files that are older than 7 days; device configuration files cannot be manually deleted from the database. (To check the current purging settings, see [Control When Device Configuration Files are Purged from the Database, on page 94](#).)



## View Archived Files for a Specific Device



**Note** If you only see a running configuration file and not a startup file, that is because the two files are the same. Cisco EPN Manager only backs up the startup configuration when it is different from the running configuration.

- Step 1** Choose **Inventory > Device Management > Configuration Archive**, then click the **Devices** tab.
- Step 2** Click a device name hyperlink. Cisco EPN Manager lists archived files according to their timestamps.

## View the Raw Content of an Archived Configuration File

Use this procedure to view the startup, running, and (if supported) VLAN, database, and admin configuration files that have been saved to the configuration archive. You can choose versions according to time stamps and then compare them with other versions.

To quickly view a device's currently-running configuration, perform a **show run** from the Device 360 view. See [View a Device's Running Configuration File \(Raw Content\)](#), on page 99.



**Note** For Cisco NCS 2000 and Cisco NCS 4000 devices, the database is backed up as a binary file. Because it is not a text file, you cannot view it or compare it with other versions, instead, you can export the file directly.

To view the contents of a running configuration file stored in the configuration archive:

- Step 1** Choose **Inventory > Device Management > Configuration Archive**, then click the **Devices** tab.
- Step 2** Click a device name hyperlink. Cisco EPN Manager lists archived files according to their timestamps.
- Step 3** Expand a time stamp to view the files that were archived at that time. You will see the details for Running Configuration, Startup Configuration, Admin Configuration, VLAN Configuration, and Database Configuration. Click the Details hyperlink under these categories, to see more information.
- Note** If you only see a running configuration file and not a startup file, that is because the two files are the same. Cisco EPN Manager only backs up the startup configuration when it is different from the running configuration.
- Step 4** Click a file under Configuration Type to view its raw data. The Raw Configuration tab lists the file contents, top to bottom.
- Step 5** To compare it with another file, click any of the hyperlinks under the Compare With column. The choices depend on the device type and number of configuration files that have been backed up to the archive. Color codes indicate what was updated, deleted, or added.



## View a Device's Running Configuration File (Raw Content)

To view a device's running configuration, execute a CLI **sh run** command from the Device 360 view **Actions** menu.

- 
- Step 1** Open the device's Device 360 view.
- Click the "i" icon next to an IP address in almost any device table
  - From the network topology, click a device in an expanded group, then click **View**
- Step 2** Choose **Actions** > **Show Command**.
- Step 3** In the Run Show Commands dialog box, choose **sh run** from the drop-down list, then click **Run**.
- 

## Label Important Configuration Files With Tags

Assigning tags to configuration files is a clear method for identifying important configurations and convey critical information. The tag is displayed with the list of files on the Configuration Archive page. Tags can also be edited and deleted using the following procedure.

- 
- Step 1** Choose **Inventory** > **Device Management** > **Configuration Archive**.
- Step 2** Locate the configuration file you want to label, and click **Edit Tag** at the top of the table.
- Step 3** Enter your content in the Edit Tag dialog box (or edit or delete existing tags) and click **Save**.
- 

## Synchronize Running and Startup Device Configurations

Devices that have startup configuration files and running configuration files may become out-of-sync (unsynchronized). A device is considered out-of-sync if its startup file (which is loaded when a device is restarted) is different from its running configuration. Unless a modified running configuration is also saved as the startup configuration, if the device is restarted, the modifications in the running configuration will be lost. The overwrite operation synchronizes the files by overwriting the device's startup configuration with its current running configuration.



---

**Note** This device configuration file synchronize operation is different from the Sync operation which performs *an immediate inventory collection for a device*. That Sync operation is described in [Collect a Device's Inventory Now \(Sync\)](#), on page 269.

---

- 
- Step 1** Identify the devices that are out-of-sync:
- a) Choose **Inventory** > **Device Management** > **Configuration Archive** .

- b) Under the Devices tab, check the Startup/Running Mismatch field .
- c) If any devices list **Yes**, make note of the devices.

**Step 2** To synchronize the devices:

- a) Click the **Archives** tab.
- b) Select the out-of-sync devices, and click **Overwrite** . (See [Overwrite a Startup Configuration with a Running Configuration, on page 102](#) for more information about the overwrite operation.)

**Step 3** To check the job details, choose **Administration > Job Dashboard** to view details about the overwrite job.

---

## Download Configuration Files

You can download the Startup and Running configuration files of up to a maximum of 1000 devices at a time, to your local system.

---

**Step 1** Choose **Inventory > Device Management > Configuration Archive**.

**Step 2** From the **Export** drop-down list, select one of the following options to download the configuration files:

1. **Sanitized**—The device credential password will be masked in the downloaded file.
2. **Unsanitized**—The device credential password will be visible in the downloaded file.

This option downloads all supported configuration from the device as a csv file. To specifically download only the Startup or the Running configuration from the device, use the alternate steps below.

The Unsanitized option appears based on the user permission set in Role Based Access Control (RBAC).

You can also download the configuration files by doing the following:

- Click the device for which you want to download configuration files in the **Inventory > Device Management > Configuration Archive** page or Click the device for which you want to download configuration files in the **Inventory > Device Management > Network Devices** page and click **Configuration Archive** tab.
  - Use the expand icon to display the required configuration details from the archive.
  - Click **Details**.
  - Select **Sanitized** or **Unsanitized** from the **Export** drop-down list.
- 

## Compare or Delete Device Configuration Files

The comparison feature displays two configuration files side by side with additions, deletions, and excluded values indicated by different colors. You can use this feature to view the differences between startup and running configuration files for out-of-sync devices, or to find out if similar devices are configured differently. You can then delete the configuration archives from the database.

Cisco EPN Manager excludes a small set of commands by default, such as the NTP clock rate (which constantly changes on a managed network element but is not considered a configuration change). You can change the

excluded commands list as described in [Specify Items to Be Excluded When Configuration Files Are Checked for Changes](#), on page 93.



**Note** File comparisons are not supported on the Cisco NCS 2000 devices because the files are saved in binary format. Only text-based files can be compared.

**Step 1** Choose **Inventory > Device Management > Configuration Archive**.

**Step 2** To delete the device configuration archive, under the Devices tab, locate the device with the configuration you want to delete and click the X delete button.

**Step 3** To compare device configuration archives:

- a) Under the Devices tab, locate the device with the configuration you want to compare and click its device name hyperlink.
- b) Expand a time stamp to view the files that were archived at that time.
- c) Launch a comparison window by clicking any of the hyperlinks under the Compare With column. The choices depend on the device type and number of configuration files that have been backed up to the archive. Color codes indicate what was updated, deleted, or added.

In the Configuration Comparison window, you can peruse the configuration by looking at the raw files or by looking at certain portions of the files (configlets). Use the color codes at the bottom window to find what was updated, deleted, or added.

## Deploy an External Configuration File to a Device

The Schedule Deploy operation updates a device's configuration file with an external file. The difference between Rollback and Schedule deploy is that the Rollback uses an existing file from the archive, while Schedule Deploy uses an external file.

Depending on the type of device, you can specify the following settings for the deploy job:

- Overwrite the current startup configuration with the new version and optionally reboot the device after the deploy.
- Merge the new file with the current running configuration and optionally archive the file as the new startup configuration.
- Schedule the deploy of database configuration files in .tgz format.

Make sure you have the location of the file on your local machine.

**Step 1** Open the device's Device Details page, from which you will execute the deploy operation.

- a) Choose **Inventory > Device Management > Network Devices**.
- b) Click the device name hyperlink to open the Device Details page.

**Step 2** Open the device's Configuration Archive page by clicking the Configuration Archive tab.

For Cisco NCS 2000 and Cisco ONS devices, this choice is displayed on the right when you click the **Chassis View** tab.

**Step 3** Click **Schedule Deploy** to open the deploy job dialog box.

**Step 4** Choose the file you want to deploy by clicking **Browse**, navigating to the file's location, and choosing the file.

**Note** To deploy database configuration files to Cisco for NCS 4000 devices, you must upload the files in .tgz format.

**Step 5** Configure the job parameters, depending on the type of file you are deploying:

- Startup configuration—Choose **Overwrite Startup Configuration**. If you want to reboot the device after the deploy operation, check the **Reboot** check box.
- Running configuration—Choose **Merge with Running Configuration**. If you want to also save the file on the device as the startup configuration, check the **Save to Startup** check box.
- Database configuration—Choose **Deploy Database Configuration** and select a database file (in .tgz format for Cisco NCS 4000 devices and .cfg format for Cisco NCS2000 devices).
- Admin configuration—Choose **Merge with Admin Configuration**.

**Step 6** Schedule the deploy job to run immediately or at a future time, and click **Submit**.

**Step 7** Choose **Administration > Job Dashboard** to view details about the image activation job.

## Overwrite a Startup Configuration with a Running Configuration

The overwrite operation copies a device's running configuration to its startup configuration. If you make changes to a device's running configuration without overwriting its startup configuration, when the device restarts, your changes will be lost.



**Note** Do not use the Overwrite button in the Archives tab (shown when you choose **Inventory > Device Management > Configuration Archive**) because it only allows you to select a device but not select a configuration file.

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

**Step 2** Click the device name hyperlink to open the device's details page, then click the Configuration Archive tab.

For Cisco NCS 2000 and Cisco ONS devices, this choice is displayed on the right when you click the **Chassis View** tab.

**Step 3** Click **Schedule Overwrite** and set the job to run immediately or at a future time, then click **Submit**.

**Step 4** Choose **Administration > Job Dashboard** to view details about the image activation job.

## Roll Back a Device's Configuration To an Archived Version

The rollback operation copies files from the archive to devices, making the new files the current configuration. You can roll back running, startup, and VLAN configurations. By default, the operation is performed by

merging the files. If you are rolling back a running configuration, you have the option to perform it using overwrite rather than merge. To roll back a configuration file to a previous version.

- Step 1** Choose **Inventory > Device Management > Configuration Archive**.
- Step 2** Click the **Archives** tab and check the device that has the configuration file you want to roll back, and click **Rollback**.
- Step 3** Choose the file types you want to roll back. In the Schedule Configuration Rollback dialog box:
- Expand the Rollback Options area.
  - From the **Files to Rollback** drop-down list, choose the file type. Choosing **All** applies the operation to startup, running, and VLAN configuration files.
- Step 4** Click the specific configuration file version that you want to roll back to.
- Step 5** Click **Schedule Rollback** and complete the following:

**Table 8: Roll Back Device Configuration**

Area	Option	Description
Rollback	Files to rollback	Select Database Configuration, Running Configuration, or Admin Configuration.
	Reboot	(Startup only) After rolling back the startup configuration, reboot the device so the startup configuration becomes the running configuration.
	Save to startup	(Running only) After rolling back the running configuration, save it to the startup configuration.
	Archive before rollback	Back up the selected file(s) before beginning the rollback operation.
	Overwrite running configuration	Overwrite (rather than merge) the old running configuration with the new one.
	Continue rollback on archive failure	(If Archive before rollback is selected) Continue the rollback even if the selected files are not successfully backed up to the database.
Rollback	Rollback Database Configuration	Begin the rollback operation for database configuration files.
Schedule	(see web GUI)	Specify whether to perform the rollback immediately or at a later scheduled time.

- Step 6** Click **Submit**.

# Export Configuration Files to a Local File System

You can export running configuration files, startup configuration files. By default, the contents of device running config files are masked when they are exported (see [Control Whether Configuration File Content Is Masked During Exports, on page 94](#)).

**Note**

For Cisco NCS 2000 devices, you can export database configurations as binary files to a file system on your local machine. With Cisco NCS 4000 devices, you can export database configurations as .tgz files. When you export it, your browser will prompt you to save or open the file.

- 
- Step 1** Choose **Inventory > Device Management > Configuration Archive**.
  - Step 2** Under the Devices tab, locate the device with the archive you want to export, and click its device name hyperlink.
  - Step 3** Locate the configuration version you want to export and expand it.
  - Step 4** Under the Configuration Type column, click the hyperlink for the file you want to export (**Running Configuration** or, if supported, **Startup Configuration**, or **Database Configuration**).
  - Step 5** In the file viewer page, click **Export** and save the file to your local machine.
- 

## Delete Archived Device Configuration Files

Provided you are a user who has the device configuration rollback privilege, you can complete one of the following procedures to manually delete archived device configuration files from the database.

**(Method 1)**

1. Choose **Inventory > Device Management > Configuration Archive**.  
The **Configuration Archive** page opens with the **Devices** tab selected.
2. From the **Name** column, click the link for the device whose configuration files you want to delete.  
Its **Archive Details** page opens.
3. Click the radio button for the configuration files you want to delete and then click the **X (Delete)** icon.
4. Click **Yes** to confirm deletion of the configuration files.

**(Method 2)**

1. Choose **Inventory > Device Management > Configuration Archive**.  
The **Configuration Archive** page opens with the **Devices** tab selected.
2. Click the **Archives** tab.
3. Check the check box for the configuration files you want to delete and then click the **X (Delete)** icon.
4. Click **Yes** to confirm deletion of the configuration files.

# Check the Network Audit for Configuration Archive Operations

To get historical information about device software image changes, check the Network Audit.

**Step 1** Choose **Inventory > Device Management > Network Audit**. To filter the results to show only image management operations, enter **archive** in the Audit Component field.

🏠 / ... / Device Management / Network Audit ★

Show Quick Filter				
Device Name	IP Address	Audit Time	Audit Component	Audit Description
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
▶ prime-asr903	209.165.200.224	2015-Jan-23 17:12:21 PST	IFM Software Image Management	Image Distribution
▶ prime-asr90	209.165.201.1	2015-Jan-23 17:11:29 PST	IFM Software Image Management	Image Distribution
▶ prime-asr	209.165.202.128	2015-Jan-23 17:11:29 PST	IFM Software Image Management	Image Distribution

**Step 2** Expand an event drawer to get details about a device change. For example, if you expand the drawer highlighted in the above figure, given in step 1, you can see that the device's running configuration file was successfully backed up to the archive at that time.

Archive configuration	<b>Success</b>
Fetch DATABASE configuration	Unsupported operation
Fetch VLAN configuration	Unsupported operation
Fetch running configuration	Success
Fetch startup configuration	Success
Syslog Message	<189>308716: *Jan 27 01:25:41.622: %SYS-5-CONFIG_I: Configured from console by vty0 (10.127.101.52)

For more information on the Network Audit feature, see [Audit Configuration Archive and Software Management Changes \(Network Audit\)](#) , on page 717.







## CHAPTER 5

# Manage Device Software Images

---

- Set Up Software Image Management, on page 107
- Copy Software Images from Devices to the Image Repository (Create a Baseline), on page 111
- How Do I Find Out Which Images Are Used by Network Devices?, on page 111
- How Do I Know a Device Has the Latest Image?, on page 112
- View the Images That Are Saved in the Image Repository, on page 112
- Find Out Which Devices Are Using an Image, on page 113
- View Recommended and Available Software Images from Cisco.com, on page 113
- How Do I Know Whether I have Permission to Download Software from Cisco.com, on page 115
- Add (Import) Software Images to the Repository, on page 115
- Change the Device Requirements for Upgrading a Software Image, on page 118
- Verify That Devices Meet Image Requirements (Upgrade Analysis), on page 118
- Distribute a New Software Image to Devices, on page 119
- Activate a New Software Image on Devices, on page 126
- Activate, Deactivate, and Remove Cisco IOS XR Images from Devices, on page 128
- View and Upgrade FPD Images, on page 129
- Commit Cisco IOS XR Images Across Device Reloads, on page 130
- Roll Back Cisco IOS XR Images, on page 130
- Check the Network Audit for Software Image Operations, on page 131
- Delete Software Image Files from the Image Repository, on page 132

## Set Up Software Image Management

- Make Sure Devices Are Configured Correctly, on page 108
- Verify the FTP/TFTP/SFTP/SCP Settings on the Cisco EPN Manager Server, on page 108
- How to Control Images that are Saved to the Image Repository During Inventory Collection, on page 108
- Adjust Criteria for Cisco.com Image Recommendations, on page 109
- Adjust Image Transfer and Distribution Preferences, on page 109
- Change Cisco.com Credentials for Software Image Operations, on page 111



---

**Note** Software Image Management is not supported on Cisco IOS-XR devices configured with a management VRF.

---

## Make Sure Devices Are Configured Correctly

Cisco EPN Manager can transfer files to and from devices only if the SNMP read-write community strings configured on your devices match the strings that were specified when the devices were added to Cisco EPN Manager. In addition, devices must be configured according to the settings in [How Is Inventory Collected?](#), on page 33.



### Note

To improve security, Cisco EPN Manager no longer uses some of the SSH CBC (Cipher Block Chaining) ciphers that older Cisco IOS-XE and IOS-XR versions use, as they have been deemed weak. For devices running Cisco IOS-XE, ensure that you upgrade to version 16.5.x or later. And for devices running Cisco IOS-XR, upgrade to version 6.1.2 or later. Otherwise, several Software Image Management operations will fail.

Although we do not recommend doing so (since it weakens security), you also have the option to add the CBC ciphers that Cisco EPN Manager stopped using back to its SSHD service configuration file. To do so, first configure the CBC ciphers in the ciphers line of the file located in the `/etc/ssh/sshd_config` directory (as shown in the example below), then restart the sshd service using the **service sshd stop/start** command.

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,
arcfour256,arcfour128,aes128-cbc,3des-cbc,
cast128-cbc,aes192-cbc,aes256-cbc
```



### Note

Software Image Management is not supported in the NAT environment. This means that image management features such as image import, upgrade, distribution, and activation, will not function in the NAT environment.

## Verify the FTP/TFTP/SFTP/SCP Settings on the Cisco EPN Manager Server

If you will be using FTP, TFTP, SFTP, or SCP make sure that it is enabled and properly configured. See [Enable FTP/TFTP/SFTP Service on the Server](#), on page 646.

## How to Control Images that are Saved to the Image Repository During Inventory Collection

Because collecting software images can slow the data collection process, by default, Cisco EPN Manager does not collect and store device software images in the image repository when it performs inventory collection. Users with Administration privileges can change that setting using the following procedure.

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **Inventory > Image Management**.
  - Step 2** To retrieve and store device images in the image repository when Cisco EPN Manager performs inventory collection, check the **Collect images along with inventory collection** check box.
  - Step 3** Click **Save**.
-

## Adjust Criteria for Cisco.com Image Recommendations

You can use Cisco.com to get information about recommended images based on criteria you provide. The following procedure shows how you can adjust those recommendations. The following table also lists the default settings.



**Note** To use these features, the device must support image recommendations.

**Step 1** Choose **Administration > Settings > System Settings**, then choose **Inventory > Image management**.

**Step 2** Adjust the recommendation settings as follows.

Setting	Description	Default
Recommend latest maintenance version of each major release	Only considers images if it is the latest maintenance version of each major release	Disabled
Recommend same image feature	Only considers images with same feature set as running device image	Disabled
Recommend versions higher than the current version	Only considers images that are higher than the running device image	Disabled
Include CCO for recommendation	Retrieves images from Cisco.com and the image repository	Enabled

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

## Adjust Image Transfer and Distribution Preferences

Use this procedure to specify the default protocols Cisco EPN Manager should use when transferring images from the software image management server to devices. You can also configure Cisco EPN Manager to perform, by default, a variety of tasks associated with image transfers and distributions—for example, whether to back up the current image before an upgrade, reboot the device after the upgrade, continue to the next device if a serial upgrade fails, and so forth. Users with Administration privileges can change that setting using the following procedure.

This procedure only sets the defaults. You can override these defaults when you perform the actual distribute operation.

**Step 1** Choose **Administration > Settings > System Settings**, then choose **Inventory > Image Management**.

**Step 2** Specify the default protocol Cisco EPN Manager should use when transferring images in the Image Transfer Protocol Order. Arrange the protocols in order of preference. If the first protocol listed fails, Cisco EPN Manager will use the next protocol in the list.

**Note** When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP for the image distribution, ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

**Step 3** Specify the default protocol Cisco EPN Manager should use when configuring images on devices in the Image Config Protocol Order area. Arrange the protocols in order of preference.

**Step 4** Specify the tasks that Cisco EPN Manager should perform when distributing images:

Setting	Description	Default
Continue distribution on failure	If distributing images to multiple devices and distribution to a device fails, continues the distribution to other devices	Enabled
TFTP fallback	Inserts the TFTP fallback command into the running image so that it can be reloaded if image distribution fails  Inserts the TFTP fallback command into the running image so that it can be reloaded if image distribution fails	Disabled
Backup current image	Before image distribution, backs up the running image to the TFTP server	Disabled
Insert boot command	After image distribution, inserts the boot command into the running image  Inserts the boot command into the running image, after image distribution	Disabled

**Step 5** Click **Save**.

## Add a Software Image Management Server to Manage Groups of Devices

To distribute images to a group of devices, add a software image management server and specify the protocol it should use for image distribution. You can add a maximum of three servers.

**Step 1** Add the server.

- Choose **Administration > Servers > Software Image Management Servers**.
- Click the Add Row icon and enter the server name, IP address, and device group the server will support.
- Click **Save**.

**Step 2** Configure the server protocol settings.

- Check the check box next to the server name, then click **Manage Protocols**.
- Click the Add Row icon and enter the software image management protocol details (username, password, and so forth).
- Click **Save**.

## Change Cisco.com Credentials for Software Image Operations

When Cisco EPN Manager connects to Cisco.com to perform software image management operations (for example, to check image recommendations), it uses the credentials stored in the Account Settings page. You can change those settings using the following procedure.

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Account Settings**.
  - Step 2** Click the **Cisco.com Credentials** tab.
  - Step 3** Change the settings, then click **Save**.
- 

## Copy Software Images from Devices to the Image Repository (Create a Baseline)

Depending on your system settings, Cisco EPN Manager may copy device software images to the image repository during inventory collection (see [How to Control Images that are Saved to the Image Repository During Inventory Collection, on page 108](#)). If you need to perform this operation manually, use the following procedure, which imports software images directly from devices into the image repository.

Before you begin, ensure that images are physically present on the devices (rather than remotely loaded).



---

**Note** If you are importing many images, perform this operation at a time that is least likely to impact production.

---

- 
- Step 1** Choose **Inventory > Device Management > Software Images**.
  - Step 2** Click the **Add/Import** tab.
  - Step 3** In the Import Images dialog box, complete the following:
    - a) In the **Source** area, select the devices (you may want to select one device group at a time).
    - b) In the **Collection Options** area, specify whether to import the files immediately or schedule the import for later.
  - Step 4** Click **Submit**.
- 

## How Do I Find Out Which Images Are Used by Network Devices?

To view a list of the images used by network devices, choose **Reports > Reports Launch Pad > Device > Detailed Software**.

To list the top ten images use by network devices (and how many devices are using those images), choose **Inventory > Device Management > Software Images**. Click **Software Image Repository** under **Useful Links**, then then click the **Image Dashboard** icon in the top-right corner of the page.

## How Do I Know a Device Has the Latest Image?

If your device type supports image recommendations, you can use the following procedure to check if a device has the latest image from Cisco.com. Otherwise, use the [Cisco.com product support pages](#) to get this information.

---

**Step 1** Choose **Inventory > Device Management > Network Devices**, then click the device name hyperlink to open the Device Details page.

**Step 2** Click the **Image** tab and scroll down to the Recommended Images area. Cisco EPN Manager lists all of the images from Cisco.com that are recommended for the device.

For Cisco NCS 2000 and Cisco ONS devices, this choice is displayed on the right when you click the **Chassis View** tab.

**Note** The recommendations list is purely informational. To use any of the recommended images, you must get them from Cisco.com and add them to the image repository. See [Add \(Import\) Software Images to the Repository, on page 115](#).

---

## View the Images That Are Saved in the Image Repository

Use this procedure to list all of the software images saved in the image repository. The images are organized by image type and stored in the corresponding software image group folder.

---

**Step 1** Choose **Inventory > Device Management > Software Images**. Cisco EPN Manager lists the images that are saved in the image repository within the **Software Image Summary** panel.

From here you can:

- Import new images into the image repository from network devices; file systems on client machines, IPv4 or IPv6 servers (URLs), FTP servers, and Cisco.com. You can use the web GUI to find out what images are available from Cisco.com, but images must be manually downloaded and then imported. See [Add \(Import\) Software Images to the Repository, on page 115](#).
- Adjust the requirements that a device must meet in order to upgrade to this image. See [Change the Device Requirements for Upgrading a Software Image, on page 118](#).
- Perform an upgrade analysis. See [Verify That Devices Meet Image Requirements \(Upgrade Analysis\), on page 118](#).
- Copy new software images to devices. See [Distribute a New Software Image to Devices, on page 119](#).
- Activate images, which makes a new image the device's running image. See [Activate a New Software Image on Devices, on page 126](#).
- Commit Cisco IOS XR images, which persists the image across device reloads and creates a rollback point. See [Commit Cisco IOS XR Images Across Device Reloads, on page 130](#).
- Delete images from the image repository (images can only be deleted using the manual process). See [Delete Software Image Files from the Image Repository, on page 132](#).

**Step 2** Go to Software Image repository and click a software image hyperlink to open the Image Information page that lists the file and image name, family, version, file size, and so forth.

From here you can:

- See which devices are using this image by checking the Device Details area at the bottom of the page.
- Adjust the requirements that a device must meet in order to upgrade to this image. (See [Change the Device Requirements for Upgrading a Software Image](#), on page 118.)

---

## Find Out Which Devices Are Using an Image

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** In the **Software Image Summary** panel, locate the image that you are interested in by expanding the image categories in the navigation area or entering partial text in one of the Quick Filter fields. For example, entering **3.1** in the Version field would list Versions 3.12.02S, 3.13.01S, and so forth.

**Step 3** Click the image hyperlink to open the Software Image Summary page. Cisco EPN Manager lists all devices using that image in the Device Details area.

---

## View Recommended and Available Software Images from Cisco.com

- [View Recommended Images on Cisco.com](#), on page 113
- [View Available Images on Cisco.com](#), on page 114

### View Recommended Images on Cisco.com

If your devices support Cisco.com image recommendations, you can use this procedure to check which images your devices should be using.

---

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** Click **Software Image Repository** under **Useful Links**.

**Step 3** Navigate to and select the software image for which you want to change requirements.

**Step 4** Choose the devices which you want to distribute the image from the **Device List** drop-down list and click **Distribution New Version**.

**Step 5** Choose one of the following image sources:

- **Recommend Image from Cisco.com** to select an image available on Cisco.com. Specify options, click **Start Recommendation**, then skip ahead to Step 5.

Cisco EPN Manager displays recommended software images for your specific device types, but it does not allow you to download software images directly from cisco.com. You must manually download software images and then import the downloaded image file.

- **Select Image from Local Repository** to select an image stored locally. Then, under Local Repository:
  - Check the **Show All Images** check box to display all images available in the image repository.
  - Uncheck the **Show All Images** check box to display the software images applicable to the selected device.

- Step 6** Select the image to distribute, then click **Apply**.
- Step 7** Choose the image name in the Distribute Image Name field to change your selection and pick a new image, then click **Save**.
- Step 8** Specify Distribution Options. You can change the default options in **Administration > System Settings > Inventory > Image Management**.
- Step 9** Specify schedule options, then click **Submit**.

## View Available Images on Cisco.com

Depending on your device type, Cisco EPN Manager can narrow the list of available images by maintenance versions, feature sets, versions, and so forth (see [Adjust Criteria for Cisco.com Image Recommendations, on page 109](#)).

Cisco EPN Manager will use the Cisco.com credentials that are set by the administrator. If default credentials are not set, you must enter valid credentials. (See [Change Cisco.com Credentials for Software Image Operations, on page 111](#)).

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** Click the **Add/Import** tab.

**Note** Although you cannot use Cisco EPN Manager to download images directly from Cisco.com and import them into the Cisco EPN Manager server, you can use the Add/Import function to check Cisco.com for available software images. Then you can manually download the images and import them into the image repository.

**Step 3** In the Import Images dialog:

- Click **Cisco.com**.
- If the credentials are not auto-populated, enter a valid Cisco.com user name and password.
- Choose a device platform and software version from the drop-down lists. The remaining choices (for example, feature type) depend on the device platform and operating system you have chosen.

**Step 4** Perform a manual download of the images by going to the Cisco.com [Software Download](#) site. Enter your credentials and follow the instructions.

**Step 5** Import the newly-downloaded images into the image repository using the procedure in [Add a Software Image from a Client Machine File System, on page 117](#).

**Step 6** Verify that the images are listed on the Software Images page (**Inventory > Device Management > Software Images**).



# How Do I Know Whether I have Permission to Download Software from Cisco.com

Cisco EPN Manager displays the recommended latest software images for the device type you specify, and it allows you to download the software images directly from Cisco.com. In order to download a EULA or K9 software image from Cisco.com, you must accept/renew the [EULA agreement](#) or [K9 Agreement](#) periodically.

Cisco EPN Manager does not display deferred software images. For detailed information, see the [Cisco EPN Manager 2.1 Supported Devices](#) list.

## Add (Import) Software Images to the Repository

Cisco EPN Manager displays the recommended latest software images for the device type you specify, and it allows you to download the software images directly from cisco.com. Cisco EPN Manager does not display deferred software images. For detailed information, see [Cisco EPN Manager 2.1 Supported Devices](#) list.

**Note**

In order to download a K9 software image from cisco.com, you must accept/renew the <https://software.cisco.com/download/eula.html> K9 agreement periodically.

The following topics explain the different ways you can add software images to the image repository. For an example of how to troubleshoot a failed import, see [Manage Jobs Using the Jobs Dashboard, on page 25](#).

- [Add a Software Image That Is Running on a Managed Device, on page 115](#)
- [Add a Software Image from an IPv4 or IPv6 Server \(URL\), on page 116](#)
- [Add a Software Image for an FTP Protocol Server \(Protocol\), on page 117](#)
- [Add a Software Image from a Client Machine File System, on page 117](#)

**Note**

For Cisco NCS and Cisco ONS devices, you can only import software images using the procedure in [Add a Software Image from a Client Machine File System, on page 117](#).

## Add a Software Image That Is Running on a Managed Device

This method retrieves a software image from a managed device and saves it in the image repository.



**Note** When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP for the image distribution, ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

Note that TFTP is supported only when copying images from the device to the server and not the other way around.

---

**Limitations:**

- For Cisco IOS-XR devices, direct import of images from the device is not supported by Cisco EPN Manager ; SMU and PIE imports are also not supported on these devices.
- For Cisco IOS-XE devices, if the device is loaded with the 'packages.conf' file, then images cannot be imported directly from that device.

---

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** Click the **Add/Import** tab.

**Step 3** In the Import Images dialog:

- Click **Device** and under Collection Options, choose one or more devices.
- In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
- Click **Submit**.

**Step 4** To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

**Step 5** Verify that the image is listed on the Software Images page (**Inventory > Device Management > Software Images**).

---

## Add a Software Image from an IPv4 or IPv6 Server (URL)

You can import software image from network-accessible IPv4 or IPv6 servers. The following file formats are supported: .bin, .tar, .aes, .pic, .mini, .vm, .gz, .ova, and .ros.

Cisco EPN Manager supports to import Non-Cisco standard image.

---

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** Click the **Add/Import** tab.

**Step 3** In the Import Images dialog:

- Click **URL**.
- In the URL To Collect Image field, enter a URL in the following format (you can also use an HTTP URL where user credentials are not required):

**http://username:password@server-ip/filename**

- In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
- Click **Submit**.

- Step 4** To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.
- Step 5** Verify that the image is listed on the Software Images page (**Inventory > Device Management > Software Images**).
- 

## Add a Software Image for an FTP Protocol Server (Protocol)

---

- Step 1** Choose **Inventory > Device Management > Software Images**.
- Step 2** Click the **Add/Import** tab.
- Step 3** In the Import Images dialog:
- Click **Protocol**.
  - Enter FTP in the Protocol field, then enter the FTP user name, password, server name or IP address, and file name. The following is a file name example:  
*/ftpfolder/asr901-universalk9-mz.154-3.S4.bin*
  - In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
  - Click **Submit**.
- Step 4** To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.
- Step 5** Verify that the image is listed on the Software Images page (**Inventory > Device Management > Software Images**).
- 

## Add a Software Image from a Client Machine File System

### Before you begin

When you import the software image file, the browser session is blocked temporarily. If the upload operation exceeds the idle timeout limit of the browser session, then you will be logged out of Cisco EPN Manager and the file import operation will be aborted. So it is recommended that you increase the idle timeout limit before you begin with this import operation. To increase the idle timeout, see [Configure the Global Timeout for Idle Users, on page 681](#).

---

- Step 1** Choose **Inventory > Device Management > Software Images**.
- Step 2** Click the **Add/Import** tab.
- Step 3** In the Import Images dialog:
- Click **File**.
  - Click the **Browse** button and navigate to the software image file.
  - In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
  - Click **Submit**.
- Step 4** To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.
- Step 5** Verify that the image is listed on the Software Images page (**Inventory > Device Management > Software Images**).
-

# Change the Device Requirements for Upgrading a Software Image

Use this procedure to change the RAM, flash, and boot ROM requirements that a device must meet for a software image to be distributed to the device. These values are checked when you perform an upgrade analysis (see [Verify That Devices Meet Image Requirements \(Upgrade Analysis\)](#), on page 118).

**Note**

This operation is not supported on the Cisco NCS 2000 and Cisco ONS families of devices.

- 
- Step 1** Choose **Inventory > Device Management > Software Images**.
- Step 2** In the **Software Image Summary** panel, locate and select the software image by clicking its associated hyperlink.
- Step 3** Click the software image name hyperlink to open its image information.
- Step 4** Adjust the device requirements:
- Minimum RAM (from 1 – 999999999999999)
  - Minimum FLASH (from 1 – 999999999999999)
  - Minimum Boot ROM Version
- Step 5** Click **Save**.
- Step 6** Click **Restore Defaults**, if you want to retain the previous requirements.
- 

## Verify That Devices Meet Image Requirements (Upgrade Analysis)

An upgrade analysis verifies that the device contains sufficient RAM or FLASH storage (depending on the device type), the image is compatible with the device family, and the software version is compatible with the image version running on the device. After the analysis, Cisco EPN Manager displays a report that provides the results by device. The report data is gathered from:

- The software image repository, which contains information about minimum RAM, minimum Flash, and so on, in the image header.
- The Cisco EPN Manager inventory, which contains information about the active images on the device, as well as Flash memory, modules, and processor details.

**Note**

Upgrade analysis is supported on all Cisco IOS-XR devices (such as Cisco NCS 1000, Cisco NCS 4000, Cisco NCS 5000, Cisco NCS 5500, and Cisco NCS 6000), except on Cisco ASR 9000 devices.

If you want to adjust the device requirements for an image, see [Change the Device Requirements for Upgrading a Software Image, on page 118](#).

- 
- Step 1** Choose **Inventory > Device Management > Software Images**.
- Step 2** Click **Upgrade Analysis** under **Useful Links**. (Do not select an image from the Software Images page.)
- Step 3** In the Upgrade Analysis dialog:
- Choose the source for the software images (the image repository or Cisco.com).
  - Select the devices you want to analyze.
  - Select the software images you want to analyze the devices against.
  - Click **Run Report**.

The report groups devices by their IP address.

---

## Distribute a New Software Image to Devices

The image distribution operation copies a new software image to a specified location on a device. You can distribute images for similar devices in a single deployment, adjusting your choices per device. When you create the job, you determine whether the job runs immediately or at a scheduled time.



---

**Note** Cisco EPN Manager does not support using TFTP to distribute images from a server to devices.

---

When you select an image to be distributed, Cisco EPN Manager only displays devices that are suitable for the image. When you create the distribution job, you specify whether Cisco EPN Manager should:

- Activate the image in the same job or skip the activation. Delaying the activation lets you perform these tasks before activating the image:
  - Find out if there is insufficient memory, clear the disk space for distributing the image or package.
  - Do an upgrade analysis to check the suitability of the device for the chosen image.
- (Cisco IOS XR only) Commit the image in the same job or skip the commit.

### Limitations:

- When you distribute image to Cisco IOS-XR devices (except Cisco ASR 9000 devices), the image is copied to the device storage before the install package is activated and committed. With Cisco ASR 9000 devices, however, the image is installed on the device directly from Cisco EPN Manager without being copied to the device storage.
- During the distribution process, if the protocols used for distribution are not supported by the device, then distribution might fail. For example, if you use the SCP protocol to distribute an image to Cisco ASR 9000 devices, then the distribution fails, because copy of the image onto the device storage is not supported in the device's command line.

The image can be distributed to any file system on the device, including folders in the root directory. This is supported only for NCS 42XX and ASR907 devices. If you choose a file system that has a stand by flash, then the image is distributed to both the active flash and the stand by flash. This means that when you choose to distribute the image to active flash, you are not required to re-distribute the image to the stand by flash.



**Note** The option to distribute an image directly to a device folder is supported only on Cisco ASR907 and Cisco NCS42xx devices.

Cisco EPN Manager displays feedback and status as the operation proceeds. If you are distributing an image to many devices, you can stagger reboots so that service at a site is not completely down during the upgrade window. For image distribution to work efficiently, the device and server from which the distribution is performed must be in the same geographical location or site. The distribution job will return an error if the distribution takes more time due to network slowness or low speed.



**Note** When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP protocol for the image distribution, ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

### Before You Begin

- When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP protocol for the image distribution, ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).
- When distributing images to Cisco ME 1200 devices, you will need to activate the image on the device immediately after distribution. Ensure that the device is ready for an image activation.

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** Click the blue **Distribute** icon in the Software Image Management Lifecycle widget. Cisco EPN Manager displays the devices that are appropriate for the images. You can configure the image for each device when you create a distribution job.

**Note** If the required device is not listed here, ensure that the Image Family associated with the file is same as the selected device's family.

To verify the device family, use the **Image** tab in the Device Details page.

**Step 3** From the **Image Selection** tab, select the image that you want to distribute on devices.

**Step 4** From the **Device Selection** tab, select the devices for image distribution. You can further adjust the distribution settings for each device.

a) In the **Image Deployment** tab, Cisco EPN Manager displays one row per device and image.

- b) For each device, check the location where the image will be copied. Cisco EPN Manager chooses the location based on its memory calculations.

**Note** Locations are not supplied for the Cisco NCS 2000 and Cisco ONS families of devices.

To change the location, double-click the location value in the **Distribute Image** field and choose another location from the drop-down list.

After you click **Save**, Cisco EPN Manager calculates whether that location has adequate space for the image. If there is enough space, Cisco EPN Manager displays a green check mark (after you click **Save**). Otherwise you must choose another location, or select the **Smart Flash Delete Before Distribution** option in step 5. Note that running images are not deleted from the device.

The following is an example of a network audit event that is generated during image distribution.

🏠 / ... / Device Management / Network Audit ★

					Show Quick Filter
Device Name	IP Address	Audit Time	Audit Component	Audit Description	
▶ prime-asr903	209.165.200.224	2015-Jan-23 17:12:21 PST	IFM Software Image Management	Image Distribution	
▶ prime-asr90	209.165.201.1	2015-Jan-23 17:11:29 PST	IFM Software Image Management	Image Distribution	
▶ prime-asr	209.165.202.128	2015-Jan-23 17:11:29 PST	IFM Software Image Management	Image Distribution	

### Step 5

From the **Image Details Verification** tab, select the file system on the device where the image must be distributed using the **Distribute Location** drop-down menu. This field displays the folders available on the device. To distribute the image to new folders, create the folder on the device manually, and return to this step. Alternatively, you can create a new folder during the distribution process automatically by choosing the 'swim\_configuration.xml' file under '/opt/CSColumos/swim' and providing any new folder name of your choice. The folder is automatically created under this directory.

### Step 6

Configure the distribution settings.

In the **Image Deployment** tab area, configure the behavior for the distribution job—for example, in a bulk distribution job, whether to continue the distribution if it fails on a device. (The preferences are populated according to defaults set by the administrator.

For more information, see [Adjust Image Transfer and Distribution Preferences, on page 109](#)).

Image Deployment Options	Cisco IOS	Cisco IOS-XE	Cisco ASR 9XX	Cisco IOS-XR	Cisco NCS 2000 and Cisco ONS 15454	Cisco NCS 4000	Cisco NCS 4200	Cisco NCS 1000	Cisco NCS 6000
<b>Back Up Current Image</b> —Back up the device's running image to the TFTP server before the new image is copied to the device	Y	Y	Y	—	—	—	Y	—	—

Image Deployment Options	Cisco IOS	Cisco IOS-XE	Cisco ASR 9XX	Cisco IOS-XR	Cisco NCS 2000 and Cisco ONS 15454	Cisco NCS 4000	Cisco NCS 4200	Cisco NCS 1000	Cisco NCS 6000
<b>Smart Flash Delete Before Distribution</b> —Delete any file (other than the running image) to recover disk space in case the device has insufficient memory (additional image files are deleted until adequate space is available in the selected flash)	Y	Y	Y	Y	—	Y	Y	Y	—
<b>Distribute Parallely</b> —Distribute images to multiple devices in parallel rather than in a serial manner	Y	Y	Y	Y	Y	Y	Y	Y	—
<b>Continue on Failure</b> —Continue the distribution even if it fails on a device	Y	Y	Y	Y	Y	Y	Y	Y	—
<b>TFTP Fallback</b> —Reload an image if the distribution fails by inserting the TFTP fallback command into the running image	Y	Y	—	—	—	—	—	—	—
<b>Insert Boot Command</b> —Insert the boot command into the running image after the image is distributed	—	Y	Y	—	—	—	Y	—	—



Image Deployment Options	Cisco IOS	Cisco IOS-XE	Cisco ASR 9XX	Cisco IOS-XR	Cisco NCS 2000 and Cisco ONS 15454	Cisco NCS 4000	Cisco NCS 4200	Cisco NCS 1000	Cisco NCS 6000
<b>ISSU</b> —Activate in-service software upgrade (ISSU) to update the software on the device with minimal service interruption	—	—	Y (Only on Cisco ASR 907)	Y	—	Y	Y (Only on Cisco NCS 4216 and Cisco NCS 4206)	—	—
<b>Only image downgrade</b> —Activate this option to distribute an image with a version lower than the version previously running on the device. This option is displayed only when the selected device supports image downgrade and it is disabled when the Activate drop-down menu is set to OFF.	—	—	—	—	Y	—	—	—	—
<b>Remove In-Active Packages after Upgrade</b> — Commit the install operation and remove previous active packages from the device repository after the device upgrade is complete.	—	—	—	—	—	Y	—	—	—

Image Deployment Options	Cisco IOS	Cisco IOS-XE	Cisco ASR 9XX	Cisco IOS-XR	Cisco NCS 2000 and Cisco ONS 15454	Cisco NCS 4000	Cisco NCS 4200	Cisco NCS 1000	Cisco NCS 6000
<b>Upgrade FPD image</b> — Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. Select this option to automatically choose FPD image packages for the upgrade during image distribution and activation processes.  Additional features include: <ul style="list-style-type: none"> <li>• Smart Flash Delete Before Distribution</li> <li>• Distribute Parallely</li> <li>• Continue on Failure</li> </ul>	—	—	—	—	—	Y	—	Y	—
<b>Interface Module Delay</b> —  Adjusts the delay between the Online Insertion and Removal (OIR) of each Interface Module (IM)	—	—	—	—	—	—	Y	—	—

**Step 7** In the **Activate Job Options** window, choose the required settings:

- Activate Options: Sequential or Parallel
- Continue on failure: Continue the distribution even if it fails on a device.
- Commit: Commit the image on the device post distribution.
- FPDs Upgrade: Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. If you enable this option, FPD image packages will be used for the upgrade.

**Step 8** Configure the image activation settings.

Device OS	Settings
Cisco IOS and Cisco IOS XE	<p>Check <b>Insert Boot Command</b> if you want the image to be activated when the device reloads, and:</p> <ul style="list-style-type: none"> <li>If you <i>do</i> want to reload the device at the end of the operation (and activate the image)—choose <b>Sequentially</b>, or <b>Parallely</b> from the drop-down list. This option is not available for Cisco IOS XE devices.</li> <li>If you <i>do not</i> want to reload the device at the end of the operation—Choose <b>OFF</b> from the drop-down list.</li> </ul> <p>If you did not check Insert Boot Command but you want to activate the image, choose <b>Sequentially</b>, or <b>Parallely</b>.</p> <p><b>Note</b> If You choose to perform an ISSU upgrade, choose <b>OFF</b> from the drop-down list. This option is only applicable to some Cisco IOS XE devices such as Cisco NCS42xx.</p>
Cisco IOS XR , Cisco NCS 2000 and Cisco ONS	<ul style="list-style-type: none"> <li>If you <i>do</i> want to activate or reload the image, choose either <b>Sequentially</b>, or <b>Parallely</b> from the drop-down list.</li> <li>If you <i>do not</i> want to activate the image, choose <b>OFF</b> from the drop-down list.</li> </ul> <p><b>Note</b> If you choose to perform an ISSU upgrade, choose <b>OFF</b> from the drop-down list. This option is applicable to all Cisco IOS XR devices.</p> <p><b>Note</b> If you choose <b>OFF</b> from the drop-down list, the <b>Only image downgrade</b> option is disabled. This option is applicable to all Cisco NCS 2000 devices.</p>

The activation options are sometimes hidden because the ability to activate images during the distribution process has been disabled in the Admin settings. To activate images, please return to **Inventory > Device Management > Software Images** and click the **Activate** icon.

**Step 9** (Cisco IOS XR devices) Configure the image commit settings. To commit the image in this job, check **Commit**. If you want to commit the image later, do not check **Commit** and then use the procedure in [Commit Cisco IOS XR Images Across Device Reloads, on page 130](#).

**Step 10** In the Schedule Distribution area, schedule the job to run immediately, at a later time, or on a regular basis.

**Step 11** Click **Submit**.

**Step 12** Choose **Administration > Job Dashboard** to view details about the image distribution job.

**Note** If the copy task takes longer than two hours, verify your connection speed from Cisco EPN Manager to the selected device.

### What to do next

If you encounter the following image distribution error, please configure the device with the commands listed and try again:

**Problem:** You encounter the error- 'ssh connections not permitted from this terminal'.

**Cause:** Device is configured incorrectly.

**Solution:** Configure the device with the following commands

```
line vty 0 <number available in the device>
    transport input ssh
    transport output ssh
```

<number available in the device> -represents the unique identifier that varies from 15 to over 100 depending on the IOS version running on the device.



**Note** These commands are not supported on Cisco IOS-XR devices.

## Activate a New Software Image on Devices



**Note** To activate Cisco IOS XR images, you can use this procedure or the procedure in [Activate, Deactivate, and Remove Cisco IOS XR Images from Devices, on page 128](#) (which performs the deactivate operation on single devices).

When a new image is activated on a device, it becomes the running image on the disk. Deactivated images are not removed when a new image is activated; you must manually delete the image from the device.

If you want to distribute and activate an image in the same job, see [Distribute a New Software Image to Devices, on page 119](#).

To activate an image without distributing a new image to a device — for example, when the device has the image you want to activate—use the following procedure. The activation uses the distribution operation but does not distribute a new image.

### Before you begin

- Before activating or reverting images on Cisco NCS 2000 devices, ensure that you disable all suppressed alarms on the device.
- If you choose the **ISSU** option to activate an image in Bundle Mode, you can verify if the device is currently in bundle mode by running this command **show version | in image** to check if the image is of the format '.bin'. You can also check the format of the image by looking at the filename of the image in the **Image** tab of the Device Details view.
- During activation using the ISSU option, if the device is in subpackage mode, for example, if the image is of the format 'bootflash:ISSU/packages.conf', ensure that you use the same folder to activate the image.

**Step 1** Choose **Inventory > Device Management > Software Images**.

**Step 2** Click the **Activate** icon in the Software Image Management Lifecycle widget.

**Step 3** **Note** You cannot perform the activation operation when the standby version is lower than the active version.

In the **Activation Source** tab, choose **Activate from Library** or **Activate from Completed Distribution Jobs** or **Activate from Standby/Alternate Images** as required.

**Step 4** If you choose Activate from Completed Distribution Jobs, click the **Activate Job Options** tab.

**Step 5** In the **Activate Job Options** window, choose the required settings and go to Step 10:

- Activate Options: Off, Sequential or Parallel
- Continue on failure: Continue the activation even if it fails on a device.
- Commit: Commit the image on the device post distribution.
- Insert boot command: Inserts the boot command into the running image after the image is distributed. This is a pre-requisite for activating devices with the ISSU option.
- Activate Options: Sequential or Parallel
- Continue on failure: Continue the distribution even if it fails on a device.
- Commit: Commit the image on the device post distribution.
- FPDs Upgrade: Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. If you enable this option, FPD image packages will be used for the upgrade.
- ISSU options:
  - Device Upgrade Mode: Your options are:
    - **Bundle Mode:** If you choose the **ISSU** option to activate an image, choose the Bundle Mode to use a monolithic Cisco IOS image to boot. This ensures that the boot variable of the device pointing to a .bin file gets the device running in the Bundle mode. If you choose this option, you must reload the device after activation. To verify if the device is in bundle mode, run this command **show version | in image** to check if the image is of the format '.bin'. You can also check the format of the image by looking at the filename of the image in the **Image** tab of the Device Details view.
    - **Install Mode:** During activation using the ISSU option, use this option if the device is in the subpackage mode, for example, if the image is of the format 'bootflash:ISSU/packages.conf', the device is run in the Install mode. Ensure that you use the same folder to activate the image. Changing the folder location will cause a failure of the activate operation. If you choose the Install Mode for a device which is already running in the Image Mode, the device is activate without reloading (ISSU) and the boot image continues to point to the packages.conf file. In all other scenarios, the devices are reloaded.
    - **Currently Exists:** If you want the device to be activated in the same mode that it is currently operating in (Install or Bundle), choose this option to activate the image using the same mode.
  - Interface Module Delay: The time (in seconds) specified in this option adjusts the delay between the Online Insertion and Removal (OIR) of each Interface Module (IM). This option is enabled only when the Insert boot command and the ISSU options are enabled, and when a supported device is selected. It is recommended to set the value of the delay to 1200 seconds or more to ensure sufficient time for the upgrade.

**Step 6** If you choose Activate from Library in the Activation Source tab, then click the **Image Selection** tab.

**Step 7** If you choose Activate from Standby Image, then go to Step 9.

**Step 8** In the **Image Selection** tab, choose the software images that you want to distribute.

**Step 9** Click the **Device Selection** tab and choose the devices for which the image must be activated.

By default, the devices for which the selected image is applicable are shown. For example, if you choose the **Activate from Standby/Alternate Images** option in Step 3, then the Device Selection tab displays only devices such as, Cisco

NCS 2000, Cisco ONS 15454 devices, and Cisco ME1200 devices, which support activation of standby/alternate images.

**Step 10** Click the **Activate Image** tab, and verify whether the selected devices and software images are mapped correctly for activation. While using standby images for activation, click the **Verify Image Selection** tab.

**Note** When you are activating a standby/alternate image, if the version of the standby/alternate image is lower than that of the image running on the device, the Verification Status Message column displays in red that you are downgrading to a lower version.

**Step 11** Click the **Activate Job Options** tab, and choose the required Activate Job options.

If you choose the **ISSU** option from the **Activate** drop-down list, the software image in the device will get upgraded without need for rebooting the device.

While activating a standby image, if the selected device supports a downgrade, then the **Only image downgrade** check box is displayed. Selecting this check box ensures that the devices are downgraded only if they support the downgrade operation (for example in case of Cisco NCS2000 devices) and any specified upgrade operation will fail.

**Step 12** Click **Submit** to activate the software image in the selected devices.

See table below for information on Cisco devices and the protocols they support for image distribution:

**Table 9: Cisco Devices and Supported Image Distribution Protocols**

Cisco Devices	TFTP	FTP	SCP	SFTP	HTTPS
Cisco ASR1000	Yes	Yes	No	Yes	No
Cisco ASR9000	Yes	No	No	Yes	No
Cisco IOS-XR (except Cisco ASR9000 devices)	Yes	Yes	Yes	Yes	No
Cisco NCS42xx, Cisco ASR9XX, or Cisco ASR 1000	Yes	Yes	Yes	No	No
Cisco ME1200	Yes	Yes	No	Yes	No
Cisco NCS2000 and Cisco ONS devices	No	Yes	No	No	Yes

## Activate, Deactivate, and Remove Cisco IOS XR Images from Devices

You can perform activate, deactivate, and delete operations on specific devices from the Device Details page. That view lists all it becomes the running image on the disk.

### Before you begin

Before activating or reverting images on Cisco NCS 2000 devices, ensure that you disable all suppressed alarms on the device.

- 
- Step 1** Open the Device Details page and click the **Image** tab.
- Step 2** Expand the **Applied Images** area to display all of the images that are installed on the device.
- Active—Images that devices are actively using.
  - Inactive—Images that are added to the boot device but are not activated.
  - Available—Images that are physically present on the device but have not been added to the boot device.
- Step 3** Identify the image you want to manage, and double-click its Status field. The field changes to an editable row.
- Step 4** Choose the operation you want to perform from the **Status** drop-down list, then click **Save**. Your options are Active, Deactivate, and Remove.
- Step 5** Click **Apply** above the images table.
- Step 6** Choose **Administration > Job Dashboard** to view details about the image activation job.
- 

## View and Upgrade FPD Images

Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. You can configure FPD image packages to be automatically chosen for the upgrade during image distribution and activation processes. Before performing an upgrade, you can view FPD details such as the device name, card type, hardware version, etc.

To do this:

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Locate and select the device with the FPD images.
- Step 3** Click the **Images** tab.
- You can now view the FPD device name, location, available card types and their hardware versions, the ATR values, the status of the image, and the running and programmed values.
- Step 4** Once you have reviewed the FPD image details, click the **Upgrade FPD Image** button, to configure the upgrade settings.
- Step 5** Schedule the upgrade to run immediately, at a later date and time, or on a regular basis.
- Step 6** Click **Submit**.
-

# Commit Cisco IOS XR Images Across Device Reloads



**Note** For Cisco IOS XR devices, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate.

When you commit a Cisco IOS XR package to a device, it persists the package configuration across device reloads. The commit operation also creates a rollback point on the device which can be used for roll back operations.

If you want to distribute, activate, and commit an image in the same job, use the procedure described in [Distribute a New Software Image to Devices, on page 119](#).

To commit an activated image, use the following procedure.



**Note** If you are only working on a single device, perform the commit operation from the Device Details page (click the **Image** tab, choose the image, and click **Commit**).

- 
- Step 1** Choose **Inventory > Device Management > Software Images**.
  - Step 2** Click the **Commit** icon in the Software Image Management Lifecycle widget.
  - Step 3** Select the devices with the image you want to commit and click **Submit**. (Images can only be committed if they have been activated.)
  - Step 4** Select the software image you want to activate, then click **Submit**.
  - Step 5** In the Schedule Distribution area, schedule the commit job to run immediately, at a later time, or on a regular basis.
  - Step 6** Click **Submit**.
  - Step 7** Choose **Administration > Job Dashboard** to view details about the image activation job.
- 

## Roll Back Cisco IOS XR Images

Rolling back a Cisco IOS XR image reverts the device image to a previous installation state—specifically, to an installation rollback point. If an image has been removed from a device, all rollback points associated with the package are also removed and it is no longer possible to roll back to that point.

A rollback job can only be performed on one device at a time. You cannot perform a rollback for multiple devices in the same job.



**Note** The rollback feature is only supported on Cisco IOS-XR devices such as Cisco ASR 9000 devices.



- Step 1** Choose **Inventory > Device Management > Network Devices**, then click the device name hyperlink for the device with the image you want to roll back.
- Step 2** Click the **Image** tab and expand the Rollback Info area.
- Step 3** Select the software image Commit ID you want to roll back to, and click **Rollback**. The Rollback Scheduler opens.
- Step 4** If you want to commit the image after the rollback operation completes, check **Commit After Rollback**.
- Step 5** In the Schedule Rollback area, schedule the rollback job to run immediately or at a later time, and click **Submit**.

## Check the Network Audit for Software Image Operations

To get historical information about device software image changes, check the Network Audit. For more information on the Network Audit feature, see [Audit Configuration Archive and Software Management Changes \(Network Audit\)](#)

- Step 1** Choose **Inventory > Device Management > Network Audit**. To filter the results to show only image management operations, enter **software image** in the Audit Component field.

🏠 / ... / Device Management / Network Audit ★

					Show <input type="button" value="Quick Filter"/>
Device Name	IP Address	Audit Time	Audit Component	Audit Description	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
▶ prime-asr903	209.165.200.224	2015-Jan-23 17:12:21 PST	IFM Software Image Management	Image Distribution	
▶ prime-asr90	209.165.201.1	2015-Jan-23 17:11:29 PST	IFM Software Image Management	Image Distribution	
▶ prime-asr	209.165.202.128	2015-Jan-23 17:11:29 PST	IFM Software Image Management	Image Distribution	

- Step 2** Expand an event drawer to get details about a device change. For example, if you expand the drawer highlighted in the above figure, you can see that the image listed in the job was successfully distributed to the device.

Device/Module ID	544544
Distribution Option : ActivatePatches	Yes
Distribution Option : BackUpCurrentImageFetch	No
Distribution Option : CfgXferProtocolOrder	TELNET, SSH
Distribution Option : Commit	No
Distribution Option : DeviceUpgradeMode	currentlyExists
Distribution Option : HaltUponError	No
Distribution Option : ISSUUpgrade	No
Distribution Option : ImgXferProtocolOrder	SCP, SFTP, FTP, TFTP
Distribution Option : InsertBootCommand	No
Distribution Option : JobDirectory	/opt/CSColumos/conf/ifm/swim/jobs
Distribution Option : RebootImmediately	No
Distribution Option : RebootMode	Sequential
Distribution Option : SCPDirectory	/localdisk/sftp
Distribution Option : SkipDistribution	No
Distribution Option : TftpDirectory	/localdisk/sftp
Distribution Option : TftpFallback	No
Distribution Option : UpgradeMode	Sequential
Distribution Option : UseSSH	Yes
Operation	Starting distribution of image to device
Running Image File Name	asr903rspl-universalk9_npe.03.13.00.S.154-3.S-ext.bin
Running Image File Name	asr903rspl-universalk9_npe.03.13.00.S.154-3.S-ext.bin

## Delete Software Image Files from the Image Repository

Software images can only be *manually* deleted from the image repository; Cisco EPN Manager does not perform any automatic purging of the image repository. If you have sufficient privileges, you can use the following procedure to delete software image files from the image repository.

- Step 1** Choose **Inventory > Device Management > Software Images**.
- Step 2** From the **Software Images Summary** panel on the left, select the images that you want to delete.
- Step 3** Click **Delete**.



## CHAPTER 6

# Perform Configuration Audits Using Compliance

- [How To Perform a Compliance Audit, on page 133](#)
- [Enable and Disable Compliance Auditing, on page 134](#)
- [Create a New Compliance Policy, on page 134](#)
- [Create Compliance Policy Rules, on page 135](#)
- [Create a Compliance Profile That Contains Policies and Rules, on page 139](#)
- [Run a Compliance Audit, on page 139](#)
- [View the Results of a Compliance Audit, on page 140](#)
- [View Violation Job Details, on page 141](#)
- [View Change Audit Details, on page 141](#)
- [View Audit Failure and Violation Summary Details, on page 142](#)
- [Fix Device Compliance Violations, on page 143](#)
- [View Audit Failure and Violation Summary Details, on page 143](#)
- [Import and Export Compliance Policies, on page 144](#)
- [View the Contents of a Compliance Policy XML File, on page 144](#)
- [View PSIRT and EoX Information, on page 145](#)

## How To Perform a Compliance Audit

The following table lists the basic steps for using the Compliance feature.

	Description	See:
1	Create a <i>compliance policy</i> that contains a name and other descriptive text.	<a href="#">Create a New Compliance Policy, on page 134</a>
2	Add rules to the compliance policy. The rules specify what constitutes a violation.	<a href="#">Create Compliance Policy Rules, on page 135</a>

3	Create a <i>compliance profile</i> (which you will use to run an audit on network devices) and: <ul style="list-style-type: none"> <li>• Add a compliance policy to it.</li> <li>• Choose the policy rules you want to include in the audit.</li> </ul> <p>You can add multiple custom policies and/or predefined system policies to the same profile.</p>	<a href="#">Create a Compliance Profile That Contains Policies and Rules, on page 139</a>
4	Run a compliance audit by selecting a profile and scheduling an audit job.	<a href="#">Run a Compliance Audit, on page 139</a>
5	View the results of the compliance audit and if necessary, fix the violations.	<a href="#">View the Results of a Compliance Audit, on page 140</a>

## Enable and Disable Compliance Auditing

The Compliance feature uses device configuration baselines and audit policies to find and correct any configuration deviations in network devices. It is disabled by default because some of the compliance reports can impact system performance. To enable the Compliance feature, use the following procedure.



### Note

To use the compliance feature, your system must meet the Professional sizing requirements, as specified in the [Cisco Evolved Programmable Network Manager Installation Guide](#).

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Server**.
- Step 2** Next to Compliance Services, click **Enable**, then click **Save**.
- Step 3** Re-synchronize the device inventory: Choose **Inventory > Network Devices**, select all devices, then click **Sync**.
- Step 4** Log out of Cisco EPN Manager and log in again to view Compliance under the **Configuration** tab.
- 

## Create a New Compliance Policy

You can create a new compliance policy starting with a blank policy template.

- 
- Step 1** Choose **Configuration > Compliance > Policies**.
- Step 2** Click the Create Compliance Policy (+) icon in the **Compliance Policies** navigation area on the left.
- Step 3** In the dialog box, enter a name and optional description, then click **Create**. The policy is added to the **Compliance Policies** navigation area on the left.
- To duplicate the policy click the **i** icon and choose **Duplicate Policy**.
-

**What to do next**

Add rules to the compliance policy. See [Create Compliance Policy Rules, on page 135](#).

## Create Compliance Policy Rules

Compliance policy rules are platform-specific and define what is considered a device violation. A rule can also contain CLI commands that fix the violation. When you are designing the compliance audit job, you can select the rules you want to include in the audit (see [Run a Compliance Audit, on page 139](#)).

Cisco EPN Manager supports audit for AireOS Wireless LAN Controllers platform.

---

**Step 1** Choose **Configuration > Compliance > Policies**, then select a policy from the navigation area on the left.

**Step 2** From the work area pane, click **New** to add a new rule.

If a similar rule exists, you can copy the rule by clicking **Duplicate**, editing the rule, and saving it with a new name.

**Step 3** Configure the new rule by entering your rule criteria.

**Note** Cisco EPN Manager supports all Java-based regular expressions. See <http://www.rexegg.com/regex-quickstart.html>.

- a) Enter a title, description, and other information in the **Rule Information** text fields. This information is free text and does not impact any of the rule settings.
- b) Specify the devices for this rule in the **Platform Selection** area.
- c) (Optional) In the **Rule Inputs** area, click **New** and specify the input fields that should be displayed to a user when they run a policy that contains this rule. For example, you could prompt a user for an IP address.

**Note** If you choose the **Accept Multiple Values** check box, the audit will pass only if all the rule inputs match in the condition.

- d) In the **Conditions and Actions** area, click **New** and specify the criteria that will be checked. This will determine the rule pass and fail conditions. For examples, see [Examples—Rule Conditions and Actions, on page 135](#).

**Step 4** Click **Create**. The rule is added to the compliance policy.

You can create as many rules as you want. Remember that when you want to run the audit job, you can pick the rules you want to validate.

---

**What to do next**

Create a profile that contains the compliance policy and its rules, and then perform the audit using the profile. See [Create a Compliance Profile That Contains Policies and Rules, on page 139](#).

## Examples—Rule Conditions and Actions

- [Example Conditions and Actions: DNS Servers Configured on Device, on page 136](#)
- [Example: Block Options, on page 136](#)
- [Example Conditions and Actions: Community Strings, on page 137](#)
- [Example Conditions and Actions: IOS Software Version, on page 138](#)

- [Example Conditions and Actions: NTP Server Redundancy, on page 138](#)

## Example Conditions and Actions: DNS Servers Configured on Device

This compliance policy checks if either **IP name-server 1.2.3.4** or **IP name-server 2.3.4.5** is configured on the device. If they are, the policy raises a violation with the message "DNS server must be configured as either 1.2.3.4 or 2.3.4.5."

Tab	Tab Area	Field	Value
Condition Details	Condition Scope Details	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	ip name-server {1.2.3.4 2.3.4.5}
Action Details	Select Match Action	Select Action	Does not raise a violation
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	DNS server must be configured as either 1.2.3.4 or 2.3.4.5

## Example: Block Options

This compliance policy checks if there are any rogue or unauthorized SNMP community strings are defined in the given blocks. If they are detected in the blocks, the policy raises a violation with the message "*Detected unauthorized community string <1.1>*" and removes all non-compliant SNMP strings from the blocks.

Tab	Tab Area	Field	Value
Rule Information		Rule Title	snmp-server community having non-standard entries
Platform Selection			Cisco IOS Devices, Cisco IOS-XE Devices
Condition 1			
Condition Details	Condition Scope Details	Condition Scope	Configuration
	Block Options	Block Start Expression	^snmp-server community .*
		(This field will be enabled only when Parse as Blocks checkbox is selected)	
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community (.*)

<b>Action Details</b>	<b>Select Match Action</b>	Select Action	Continue
	<b>Select Does Not Match Action</b>	Select Action	Does Not Raise a Violation
<b>Condition 2</b>			
<b>Condition Details</b>	<b>Condition Scope Details</b>	Condition Scope	Previously Matched Blocks
	<b>Block Options</b>	Block Start Expression (This field will be enabled only when Parse as Blocks checkbox is selected)	^snmp-server community .*
	<b>Condition Match Criteria</b>	Operator	Matches the expression
		Value	snmp-server community ((public RO) (private RW))
<b>Action Details</b>	<b>Select Match Action</b>	Select Action	Continue
	<b>Select Does Not Match Action</b>	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Detected unauthorized community string <1.1>.

**Note**

In the above example, the matching criteria will be termed as 1.1, 1.2, and so on, for first condition. For the second condition, the matching criterial will be termed as 2.1, 2.2, and so on.

## Example Conditions and Actions: Community Strings

This compliance policy checks if either **snmp-server community public** or **snmp-server community private** is configured on a device (which is undesirable). If it is, the policy raises a violation with the message "Community string xxxxx configured", where xxx is the first violation that was found.

Tab	Tab Area	Field	Value
<b>Condition Details</b>	<b>Condition Scope Details</b>	Condition Scope	Configuration
	<b>Condition Match Criteria</b>	Operator	Matches the expression
		Value	snmp-server community {public private}

<b>Action Details</b>	<b>Select Match Action</b>	Select Action	Raise a violation
	<b>Select Does Not Match Action</b>	Select Action	Continue
		Violation Message Type	User Defined Violation Message
		Violation Text	Community string xxxxx configured.

## Example Conditions and Actions: IOS Software Version

This compliance policy checks if Cisco IOS software version **15.0(2)SE7** is installed on a device. If it is not, the policy raises a violation with the message "Output of show version contains the string xxxxx," where xxxxx is the Cisco IOS software version that does not match 15.0(2)SE7.

Tab	Tab Area	Field	Value
<b>Condition Details</b>	<b>Condition Scope Details</b>	Condition Scope	Device Command Outputs
		Show Commands	show version
	<b>Condition Match Criteria</b>	Operator	Contains the string
		Value	15.0(2)SE7
<b>Action Details</b>	<b>Select Match Action</b>	Select Action	Continue
	<b>Select Does Not Match Action</b>	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Output of show version contains the string xxxxx.

## Example Conditions and Actions: NTP Server Redundancy

This compliance policy checks if the command **ntp server** appears at least twice on the device. If it does not, the policy raises a violation with the message "At least two NTP servers must be configured."

Tab	Tab Area	Field	Value
<b>Condition Details</b>	<b>Condition Scope Details</b>	Condition Scope	Configuration
	<b>Condition Match Criteria</b>	Operator	Matches the expression
		Value	(ntp server.*\n){2,}



Action Details	Select Match Action	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	At least two NTP servers must be configured.

## Create a Compliance Profile That Contains Policies and Rules

A compliance profile contains one or more compliance policies. When you add a compliance policy to a profile, all of the policy's rules are applied to the profile. You can customize the profile by selecting the policy rules you want to include (and ignoring the others). If you group several policies in a profile, you can select and deselect the rules for each policy.

**Step 1** Choose **Configuration > Compliance > Profiles**.

**Step 2** Click the Create Policy Profile (+) icon in the **Compliance Profiles** navigation area on the left. This opens the **Add Compliance Policies** dialog box.

**Step 3** Select the policies you want to include in the profile. User defined policies will be available under the User Defined category.

- a) In the **Add Compliance Policies** dialog box, choose the policies you want to add.
- b) Click **OK**. The policies are added to the **Compliance Policy Selector** area.

**Step 4** Select the rules you want to include in the policy.

- a) Select a policy in the **Compliance Policy Selector** area. The policy's rules are displayed in the area on the right.
- b) Select and deselect specific rules, then click **Save**.

**Note** The choices you make here only apply to the *policy instance in this profile*. Your choices do not modify the original version of the compliance policy.

### What to do next

Schedule the compliance audit job as described in [Run a Compliance Audit, on page 139](#).

## Run a Compliance Audit

To run a compliance audit, select a profile, choose the devices you want to audit (using the policies and rules in the profile), and schedule the audit job.

**Step 1** Choose **Configuration > Compliance > Profiles**.

**Step 2** Select a profile in the **Compliance Profiles** navigation area on the left.

**Step 3** Click the Run Compliance Audit icon in the **Compliance Profiles** navigation area.

- Step 4** Expand the **Devices and Configuration** area, select the required devices and configuration files that you want to audit.
- Select the devices (or device groups).
  - Specify which configuration file you want to audit.
    - **Use Latest Archived Configuration**—Audit the latest backup file from the archive. If no backup file is available, Cisco EPN Manager does not audit the device.
    - **Use Current Device Configuration**—Poll and audit the device's running configuration. (For example, show command output will be from the device's running configuration.)

When you select this option, Cisco EPN Manager first takes a backup of the configuration from device and then performs audit. This is useful when periodic or event triggered configuration backup is not enabled and also useful because archived configuration in Cisco EPN Manager is often out-of-sync with the device.
  - Click **Next**.
- Step 5** Select **Now** to schedule the audit job immediately or select **Date** and enter a date and time to schedule it later. Use the **Reccurrence** option to repeat the audit job at regular intervals.
- Step 6** Click **Finish**. An audit job is scheduled. To view the status of the audit job, choose **Configuration > Compliance > Jobs**.

### What to do next

Check the audit results as described in [View the Results of a Compliance Audit, on page 140](#).

## View the Results of a Compliance Audit

Use this procedure to check an audit job results. The results will tell you which devices were audited, which devices were skipped, which devices had violations, and so forth. There might be several different compliance policies running on a single device.

After a job is created, you can set the following preferences for the job:

- **Pause Series**—Can be applied only on jobs that are scheduled in the future. You cannot suspend a job that is running.
- **Resume Series**—Can be applied only on jobs that have been suspended.
- **Edit Schedule**—Reschedule a job that has been scheduled for a different time.

**Step 1** Choose **Configuration > Compliance > Jobs**.

**Step 2** Click the **Audit Jobs** tab, locate your job, and check the information in the **Last Run** column.

Last Run Result Value	Description
Failure	One or more devices audited have a violation in the policies specified in the profile.
Partial Success	The compliance job contains a mix of both audited and non-audited devices, and the compliance status of audited devices is successful.

Success	All devices audited conform to the policies specified in the profile.
---------	-----------------------------------------------------------------------

For a compliance audit job, the number of violations supported is 20000 for Standard setup and 80000 for Pro and above setup of Cisco EPN Manager .

**Step 3** If the audit check failed:

- To see which devices failed, hover over the "i" icon next to the **Failure** hyperlink to display a details popup.
- Launch a Device 360 view by selecting the job, clicking **View Job Details**, and clicking the "i" icon next to a device in the popup window.

**Step 4** For the most detail, click the **Failure** hyperlink to open the **Compliance Audit Violation Details** window.

**Note** Use the **Next** and **Previous** buttons to traverse the **Compliance Audit Violation Details** window.

- Check the **Job Details and Violations** area for a summary of the failures. The fields are described in the section *Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs* in [Cisco Prime Infrastructure Field Reference](#) (the content is applicable to Cisco EPN Manager ).
- Check the **Violations by Device** area for per-device details.

### What to do next

To fix any of the violations, see [Fix Device Compliance Violations, on page 143](#).

## View Violation Job Details

The following table shows the details that can be viewed from the Violation Details page.

To View:	Do the following
The status of scheduled fixable violation jobs.	<ol style="list-style-type: none"> <li>1. Go to the <b>Violation Details</b> page.</li> <li>2. Click the <b>Fixable</b> column filter box and choose <b>Running</b>.</li> </ol>
The details of Fixed violation jobs.	<ol style="list-style-type: none"> <li>1. Go to the <b>Violation Details</b> page.</li> <li>2. Click the <b>Fixable</b> column filter box and choose <b>Fixed</b>.</li> <li>3. Click the <b>Fixed</b> link.</li> </ol>
The details of Fix Failed violation jobs.	<ol style="list-style-type: none"> <li>1. Go to the <b>Violation Details</b> page.</li> <li>2. Click the <b>Fixable</b> column filter box and choose <b>Fix Failed</b>.</li> <li>3. Click the <b>Fix Failed</b> link.</li> </ol>

## View Change Audit Details

**Step 1** Log in to Cisco EPN Manager as an administrator

**Step 2** Choose **Monitor > Tools > Change Audit Dashboard**.

The **Change Audit Dashboard** displays the network audit logs and change audit data of device management, user management, configuration template management, device community and credential changes, and inventory changes of devices. The **Change Audit report** and **Change Audit** dashboard display the details irrespective of the virtual domain you are logged in.

## View Audit Failure and Violation Summary Details

You can view detailed violation information, export this data, and view details of compliance jobs. You can export detailed data for a specific job, or export summary data for multiple jobs.

**Step 1** Choose **Configuration > Compliance > Jobs**.

**Step 2** To view the details for a specific audit job:

- a) Click the **Audit Jobs** tab and locate your job.
- b) Click the job's **Failure** hyperlink to view the **Compliance Audit Details** window.

You can view information about the policy name, the set rules, its compliance state, the total violation count, the job's instance count, its highest severity value, and the ignored count values.

- c) To export these details use one of the following options:
  - To export the violation details to a Microsoft Excel spreadsheet in XLS format, click **Export as XLS**.
  - To export the violation details to a Microsoft Excel spreadsheet in comma-separated text, click **Export as CSV**.
  - To export the violation details to an HTML file, click **Export as HTML**.
- d) Click **Save File**.

**Step 3** To view a collective summary of all audit jobs:

- a) Click the **Violation Summary** tab.

You can view a collective report for all devices on which violations have occurred, their associated policy and profile names, their audit job IDs, their associated rules and rule severity values, details on whether the violations are fixable or not, or whether they are already fixed, and the message associated with the violation.

- b) To export this detailed summary report, choose one of the following options from the drop-down menu:
  - To export the summary to a Microsoft Excel spreadsheet in comma-separated text, click **Violation Report CSV**.
  - To export the summary to a PDF file, click **Violation Report PDF**.
- c) Click **Save File**.

### What to do next

To fix any of the violations, see [Fix Device Compliance Violations, on page 143](#).

# Fix Device Compliance Violations

Use this procedure to fix compliance violations for a failed compliance audit.

- 
- Step 1** Choose **Configuration > Compliance > Jobs**.
- Step 2** Click the **Audit Jobs**, locate your job, and check the information in the **Last Run Result** column.
- Step 3** Click the **Failure** hyperlink to open the **Compliance Audit Violation Details** window.
- Note** Use the **Next** and **Previous** buttons to traverse the **Compliance Audit Violation Details** window.
- Step 4** In the **Job Details and Violations** area, click **Next**.
- Step 5** In the **Violations by Device** area, select the device and violation and click **Next**.
- Step 6** In the **Fix Rule Inputs** area, preview the fix commands that were previously defined in the policy, then click **Next**.
- If custom policies are created with `fix cli ^<Rule input ID>^` as the action for the condition, then the Fix Rule Inputs tab is displayed. Enter the required fix rule values and click **Next** to continue.
- Step 7** Review the configuration that is displayed in the Preview Fix Commands pop up.
- Step 8** Schedule the fix job so that the generated configuration can be deployed to the device, then Click **Schedule the Fix Job**.
- 

## What to do next

To view any of the violations job details, see [View Audit Failure and Violation Summary Details, on page 142](#).

# View Audit Failure and Violation Summary Details

You can view detailed violation information, export this data, and view details of compliance jobs. You can export detailed data for a specific job, or export summary data for multiple jobs.

- 
- Step 1** Choose **Configuration > Compliance > Jobs**.
- Step 2** To view the details for a specific audit job:
- Click the **Audit Jobs** tab and locate your job.
  - Click the job's **Failure** hyperlink to view the **Compliance Audit Details** window.
- You can view information about the policy name, the set rules, its compliance state, the total violation count, the job's instance count, its highest severity value, and the ignored count values.
- To export these details use one of the following options:
    - To export the violation details to a Microsoft Excel spreadsheet in XLS format, click **Export as XLS**.
    - To export the violation details to a Microsoft Excel spreadsheet in comma-separated text, click **Export as CSV**.
    - To export the violation details to an HTML file, click **Export as HTML**.

d) Click **Save File**.

**Step 3** To view a collective summary of all audit jobs:

a) Click the **Violation Summary** tab.

You can view a collective report for all devices on which violations have occurred, their associated policy and profile names, their audit job IDs, their associated rules and rule severity values, details on whether the violations are fixable or not, or whether they are already fixed, and the message associated with the violation.

b) To export this detailed summary report, choose one of the following options from the drop-down menu:

- To export the summary to a Microsoft Excel spreadsheet in comma-separated text, click **Violation Report CSV**.
- To export the summary to a PDF file, click **Violation Report PDF**.

c) Click **Save File**.

---

#### What to do next

To fix any of the violations, see [Fix Device Compliance Violations, on page 143](#).

## Import and Export Compliance Policies

Compliance policies are saved as XML files. You can export individual compliance policies and, if desired, import them into another server. Files can only be imported in XML format.

---

**Step 1** Choose **Configuration > Compliance > Policies**.

**Step 2** To export a compliance policy:

- Mouse hover on "i" icon next to the policy in the **Compliance Policies** navigation area on the left.
- In the popup window, click the **Export Policy as XML** hyperlink, and save the file.

**Step 3** To import a compliance policy:

- Click the Import Policies icon above the **Compliance Policies** navigation area on the left.
- In the **Import Policies** dialog box, click **Choose Policies**.
- Browse to the XML file and select it.
- Click **Import**.

---

## View the Contents of a Compliance Policy XML File

Compliance policies are saved as XML files. To view the contents of a policy's XML file:

---

**Step 1** Choose **Configuration > Compliance > Policies**.

**Step 2** Locate the policy in the **Compliance Policies** navigation area on the left, then hover your mouse over the "i" icon next to the policy.

- Step 3** In the popup window, click the **View Policy as XML** hyperlink. Cisco EPN Manager displays the content in XML format.
- 

## View PSIRT and EoX Information

- [View Device Security Vulnerabilities](#) , on page 145
- [View Device Hardware and Software End-of-Life Report](#) , on page 145
- [View Field Notices for Device](#) , on page 146

## View Device Security Vulnerabilities

You can run a report to determine if any devices in your network have security vulnerabilities as defined by the Cisco Product Security Incident Response Team (PSIRT). The report includes Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Notice information. You can also view documentation about the specific vulnerabilities that describes the impact of a vulnerability and any potential steps needed to protect your environment.



**Note** PSIRT and EoX reports cannot be run for specific devices. When you schedule PSIRT and EoX jobs, the report is generated for all devices in Managed and Completed state (on the **Inventory > Configuration > Network Devices** page).

---

### Before you begin

Sync the devices prior to scheduling the job. Choose **Configuration > Network Devices**, select the devices, then click **Sync**.

---

**Step 1** Choose **Reports > PSIRT and EoX**.

**Step 2** Schedule and run the job.

A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. Separate jobs on each of the tabs need not be created.

**Step 3** Click **View Job Details** to view the current status of the PSIRT report.

**Step 4** When the report is completed, click the **Device PSIRT** tab to view PSIRT information.

**Step 5** In the **PSIRT Title** column, click the hyperlink to view the full description of a security vulnerability.

**Step 6** (Optional) You can export the device PSIRT details in PDF and CSV format for each device and for all devices collectively.

---

## View Device Hardware and Software End-of-Life Report

You can run a report to determine if any Cisco device hardware or software in your network have reach edits end of life (EOX). This can help you determine product upgrade and substitution options.

- 
- Step 1** Choose **Reports > PSIRT and EoX**.
- Step 2** Click **Schedule Job**. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.
- Step 3** After the job completes, click one of the following EOX tabs to view the report information specific to that tab:
- **Device Hardware EOX**
  - **Device Software EOX**
- Step 4** (Optional) You can export these device EoL details in PDF and CSV format for each device and for all devices collectively.
- 

## View Field Notices for Device

You can run a report to determine if any Cisco devices that are managed and have completed a full inventory collection have any field notices. Field Notices are notifications that are published for significant issues, other than security vulnerability-related issues, that directly involve Cisco products and typically require an upgrade, workaround, or other customer action.

- 
- Step 1** Choose **Reports > PSIRT and EoX**.
- Step 2** Click **Schedule Job**. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.
- Step 3** Click the **Field Notice** tab to view field notice information.
- Step 4** Click on the hyperlink in the Field Notice Name column to view more information on cisco.com.
- Step 5** (Optional) You can export the device field notice details in PDF and CSV format for each device and for all devices collectively.
-





## PART III

# Visualize the Network

- [Visualize the Network Topology, on page 149](#)





## CHAPTER 7

# Visualize the Network Topology

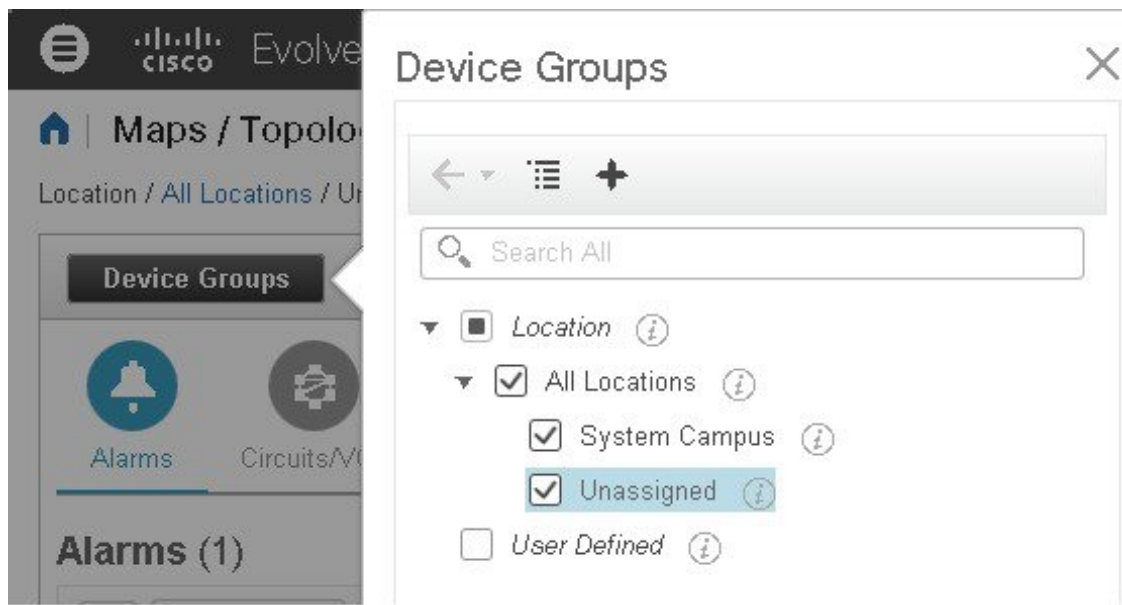
This chapter provides the following topics:

- [Network Topology Overview, on page 149](#)
- [View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map, on page 151](#)
- [Search for a Device in the Map, on page 153](#)
- [Determine What is Displayed in the Topology Map, on page 153](#)
- [Get More Information About Devices, on page 160](#)
- [Get More Information About Links, on page 160](#)
- [Troubleshoot Link Issues, on page 165](#)
- [Show Bandwidth Utilization for Links on the Map, on page 166](#)
- [View Fault Information for Devices and Links, on page 169](#)
- [Change the Layout of a Network Topology Map, on page 169](#)
- [Add a Background Image to the Network Topology, on page 171](#)
- [Visualize and Trace Circuits/VCs, on page 171](#)
- [Show Clock Synchronization Networks on a Network Topology Map, on page 172](#)
- [Show Routing Networks on the Topology Map, on page 173](#)
- [Save the Topology Map as an Image File, on page 174](#)
- [View Your Network on a Geographical Map \(Geo Map\), on page 175](#)

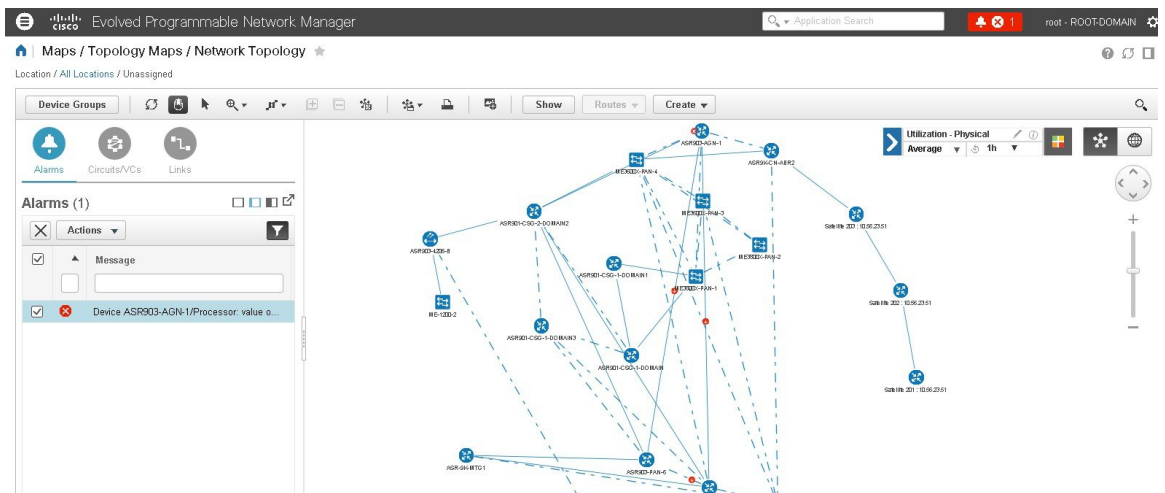
## Network Topology Overview

The Network Topology window presents a graphical, topological map view of devices, the links between them, and the active alarms on elements in the map. It also enables you to visualize circuits/VCs within the displayed topology map. In addition, the Network Topology window provides access to map element tools and functions, and allows you to drill-down to get detailed information about map elements.

The Network Topology window is accessed from the left sidebar (**Maps > Topology > Network Topology**). The content of the Network Topology window is determined by the device group(s) you have selected. To select a device group, click the Device Groups button in the toolbar and select one or more groups in the Device Groups panel. (From the Device Groups panel you can access the central device grouping functionality to create new groups, add devices to groups, and so on. See [Create Groups of Devices for Easier Management and Configuration, on page 55](#) for more information. )



Each Network Topology map is divided into a left pane that contains alarms/circuits/VCs/links information, and a right pane that displays the map itself. From the left pane, use the toolbar to control the spacing of both panes. For example, if you select 100%, only the map will be shown. If you select 50%, the map and the left pane will share the screen equally. When the left pane is expanded, additional columns might be added to the tables in the tabs.



- Alarms, Circuits/VCs, and Links (left pane)—Provides information relevant to the devices and topology shown in the map.
  - Alarms tab—Shows a table listing the current alarms for the selected group(s) and their severity. You can select alarms and perform basic actions, such as clear, acknowledge, and so on. For full details of the alarms, click the Alarms Table link at the bottom of the Alarms tab.
  - Circuits/VCs tab—Lists the circuits/VCs relevant to the devices in the selected group(s), and indicates the primary state of each circuit/VC. The primary state reflects the most serious current state of the circuit, as derived from the provisioning, serviceability, discovery, and alarm states. See [Circuit or](#)

[VC States, on page 520](#). By default, the circuits/VCs are sorted by primary state, from most to least severe. Note that:

- Selecting a circuit/VC in the list displays a visual representation of the circuit/VC in the topology map.
- Clicking the Circuits/VCs link at the bottom of the tab launches a separate window with a table of circuits/VCs providing more details for each circuit/VC.
- Clicking the Network Interfaces link at the bottom of the tab launches a table listing the interfaces that have been configured for participation in circuits/VCs, such as UNIs and ENNIs.
- Clicking the appropriate toolbar icon allows you to perform actions such as creating a new circuit or running an ITU-T Y.1564 test on the selected circuit.
- Links tab—Lists the links relevant to the selected device group(s) and shows the highest severity alarm on the link. Selecting a link in the table highlights the link in the topology map. Clicking the Links Table link at the bottom of the tab launches a separate window with a table of links.
- Topology map (right pane)—Displays the topology of the selected device group(s) in graphical form. It displays the group's devices and sub-groups (if any) and the links between them (Physical, Ethernet, and technology-specific links). It also displays the active alarms on the devices or links so that you can easily identify problems in the network. You can drill down from the topology map to detailed information about a device or link in order to troubleshoot problems. The topology map can be customized, filtered, and manipulated to show exactly the information you need.

You can toggle between the network topology map and the geographical map using the toggle buttons in the top right corner of the map.

## View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map

From the Network Topology window, you can access extended tables that list and provide more information about the alarms, network interfaces, circuits/VCs and links in the selected device group. These extended tables open in a separate browser window.

The tables accessed from the Network Topology window contain information for the selected device group only. You can access a full list of all alarms/circuits/deleted circuits/network interfaces/links in the system by selecting **Inventory > Other** and then selecting the required table (links, network interfaces, and so on).

To open the extended details tables, click the **Detach** icon in the top right corner of the tab or click on the hyperlink at the bottom of a specific tab, for example, click on the Alarms Table link at the bottom of the Alarms tab.

The window displaying the extended tables has these tabs: Alarms, Circuits/VCs, Deleted Circuits/VCs, Network Interfaces, and Links.

**Location/All Locations/Unassigned**

Alarms Circuits/VCs Deleted Circuits/VCs Network Interfaces Links

Change Status ▾ Assign ▾ Annotation ▾ X Delete Email Notification Troubleshoot ▾

<input type="checkbox"/>	Severity	Message	Status	Failure Source	Timestamp ▾	Device Ti...	Owner
<input type="checkbox"/>	Critical	TL1 Session for a...	Not Acknowled...	TL1 Session Fa...	March 15, 2017...		
<input type="checkbox"/>	Critical	TL1 Session for a...	Not Acknowled...	TL1 Session Fa...	March 15, 2017...		
<input type="checkbox"/>	Critical	TL1 Session for a...	Not Acknowled...	TL1 Session Fa...	March 15, 2017...		
<input type="checkbox"/>	Critical	TL1 Session for a...	Not Acknowled...	TL1 Session Fa...	March 15, 2017...		
<input type="checkbox"/>	Critical	TL1 Session for a...	Not Acknowled...	TL1 Session Fa...	March 15, 2017...		
<input type="checkbox"/>	Critical	TL1 Session for a...	Not Acknowled...	TL1 Session Fa...	March 15, 2017...		
<input type="checkbox"/>	Critical	TL1 Session for a...	Not Acknowled...	TL1 Session Fa...	March 15, 2017...		
<input type="checkbox"/>	Warning	Alarm synchroniza...	Not Acknowled...	TL1 Alarm Syn...	March 15, 2017...		
<input type="checkbox"/>	Critical	TL1 Session for a...	Not Acknowled...	TL1 Session Fa...	March 15, 2017...		
<input type="checkbox"/>	Minor	I2C access error	Not Acknowled...	NCS4k-B 0/...	March 15, 2017...	March 5,...	
<input type="checkbox"/>	Minor	I2C access error	Not Acknowled...	NCS4k-B 0/...	March 15, 2017...	March 5,...	

Be aware of the following when working with the extended tables:

- When the extended tables window is open, the left pane of the Network Topology window is disabled. When you close the extended tables window, the tabs in the left pane of the Network Topology window become fully functional again.
- There is synchronization between the extended tables and the corresponding tabs in the Network Topology window. For example, if you select a circuit/VC in the extended Circuits/VCs table, that circuit will also be selected in the Circuits/VCs tab in the Network Topology window and the circuit/VC overlay will be shown in the topology map. Conversely, if you select a circuit/VC in the Network Topology window and then open the extended table, the same circuit/VC will be selected in the extended table.
- Alarms and circuits/VCs in both the Network Topology window and in the extended tables are refreshed based on the user preference settings. See [Set Up Your Alarm and Event Display Preferences, on page 218](#) and [Customize the Alarm Summary, on page 220](#).
- Click the **Export** icon at the top right of the table to export the data from the table to a file (either PDF or CSV format). Export is available for alarms, circuits/VCs and network interfaces.



**Note** If the table contains more than 1000 rows, you will not be able to export the data.

- Click the *i* icon next to the **Provisioning** column in the Circuits/VCs and Deleted Circuits/VCs tabs to view the details of configuration, configuration errors, rollback configuration, and rollback configuration errors for each device participating in the circuit/VC. The *i* icon is available for all provisioning states, except None.

## Filter Data in the Detailed Tables

You can also filter the data to find specific alarms, circuits/VCs, network interfaces, or links using a *quick filter* or an *advanced filter* from the **Show** drop-down list. The quick filter narrows the content that is displayed in a column according to the text you enter above the column. The advanced filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. You can also create a *user defined* filter which, if saved, will be added to the **Show** drop-down menu.

To create and save a user defined filter:

- 
- Step 1** From the **Show** drop-down list above the extended tables of alarms, circuits/VCs, network interfaces, and links, choose **Advanced Filter**.
- Step 2** In the **Advanced Filter** data popup window, enter the advanced filter criteria, and then click **Save As**.
- Step 3** In the **Save Filter** dialog box, enter a name for your filter and click **Save**.
- To edit or remove a user defined filter, choose **Manage User Defined Filters** from the **Show** drop-down list.
- 

## Search for a Device in the Map

You can search for devices in the topology map and in the geo map by the following criteria:

- Device name
- Device family
- IP address
- User defined field value

To search for specific devices in the map:

- 
- Step 1** Click the **Search** icon in the toolbar.
- Step 2** Type the full or partial device name/IP address/device family/user defined field value in the search text box and press **Enter**. In the topology map, you will see a list of devices that match the search criteria. In the geo map, the Search Results panel lists the devices that match your search and indicates whether they are mapped or unmapped. Click on the **i** icon to show the Device 360 which contains more information about the device. Click on a device to highlight it in the map.
- 

## Determine What is Displayed in the Topology Map

- [Choose Which Device Group\(s\) to Display in the Network Topology Map, on page 154](#)
- [View the Contents of a Sub-Group in the Topology Map, on page 154](#)
- [Manually Add Links to the Topology Map, on page 156](#)
- [Change Which Link and Device Types are Shown in the Network Topology Map, on page 157](#)



- [Show/Hide Alarms and Labels in the Topology Map, on page 158](#)
- [Isolate Specific Sections of a Large Topology Map, on page 159](#)

## Choose Which Device Group(s) to Display in the Network Topology Map

The topology map enables you to visualize the topology of a device group or multiple device groups. The selected group(s) might cover a specific network segment, a customer network, or any other combination of network elements. Device grouping is hierarchical. There are two top-level parent groups containing multiple sub-groups - Location groups and User Defined groups. You can display multiple groups within the same top-level parent group. For example, you can display multiple Location groups but you cannot display one Location group and one User Defined group.

To determine which devices are displayed in the topology map, click on the **Device Groups** button in the left pane and select one or more device groups.

After you have displayed the required group(s) in the topology map, you can access additional information about any device or link. See [Get More Information About Devices](#) and [Get More Information About Links](#)

The topology map only displays devices for which the logged in user has access privileges, based on the virtual domains to which the user has been assigned.



### Note

If you encounter topology issues, such as topology components not rendering as expected or component data not being displaying on the map, we recommend that you clear your browser cache and try again.

To display network elements in the topology map:

- 
- Step 1** Choose **Maps > Topology Maps > Network Topology**.
  - Step 2** Click on the **Device Groups** button in the left pane to open the Device Groups panel.
  - Step 3** Click on the device group(s) you want to display in the topology map and click **Load**. The device group selections are displayed above the topology map.
  - Step 4** Customize the topology map as required by showing specific device/link types, adding manual links, and so on. See the following topics for more information:
    - [Change Which Link and Device Types are Shown in the Network Topology Map, on page 157](#)
    - [Manually Add Links to the Topology Map, on page 156](#)
    - [Change the Layout of a Network Topology Map, on page 169](#)
- 

## View the Contents of a Sub-Group in the Topology Map

You can expand a sub-group to show its contents within the current context or you can drill down to see the contents of the sub-group independently of the current map context.





**Note** When expanding sub-groups, be aware that if a device belongs to more than one group, the device will appear in one of the expanded groups only. It will not appear in all of the groups to which it belongs. If your setup has devices that belong to multiple groups, rather view the groups individually in the topology map by selecting them in the Device Groups pane. This will ensure that you will always see all the devices that belong to a specific group.

To view the contents of a sub-group:

**Step 1** Click on a sub-group in the topology map.

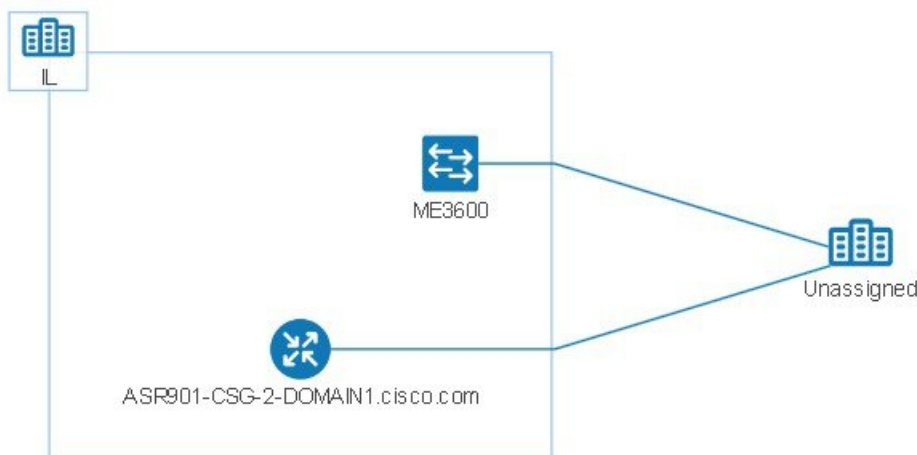
**Step 2** In the displayed popup, click one of the following:

- **Drill down group**—Displays the sub-group on its own in the topology map, meaning that the currently displayed group is replaced with the selected sub-group. Note that the sub-group name is selected in the Device Groups pane.

**Note** You can double-click on the sub-group to quickly drill down into the group.

- **Expand group**—Adds the contents of the sub-group to the current topology map display.

In the figure below, the IL group is expanded.



## Manually Add Devices and Networks to the Topology Map

You can display devices and networks that are not managed by the system on the topology map and on the geo map by adding them manually.

**Step 1** In the topology toolbar, choose **Create > Create Unmanaged Device** or **Create > Create Unmanaged Network**.

**Step 2** Click on the map to add the device/network to the map.

**Step 3** Click on the newly-added device/network in the map. From the displayed panel, you can add the device/network to a group, rename the device/network, or delete the device/network.

After you have added a device or network to the topology map, it will also be available in the geo map. The unmanaged device will appear in the list of unmapped devices and you can set its location. See [Place Unmapped Devices on the Geo Map, on page 178](#).

---

## Manually Add Links to the Topology Map

If you know that two devices are connected but Cisco EPN Manager cannot discover the link and show it on the map, you can add the link manually. After you add this link, it will be shown by default whenever the relevant group is shown on the map.



---

**Note** This feature is supported for optical OCH links only.

---

You can add the following types of manual links:

- **Unmanaged links:** For visualization purposes only. If you know that two devices are connected but you do not need full management of the link between them, you can add an unmanaged link to the map. The link will appear as a grey dashed line.
- **Managed links:** When you add a managed link, it is saved to the database and is included in all links tables. It is shown on the map as a solid line, the same as all other managed links. Cisco EPN Manager retrieves the link status from the managed device interfaces to which it is connected. The discovery status of a manually added managed link will be "Pre-provisioned." This indicates that it was not discovered by the system.

To manually add a link between two devices:

- 
- Step 1** In the topology toolbar, choose **Create > Create Unmanaged Link** or **Create > Create Managed Link**.
- Step 2** Click and hold down the mouse on the first device in the topology map and drag it to the second device.
- Step 3** In the Interface Details dialog, select the source interface on the first device and the target interface on the second device from the drop-down lists of available interfaces, and click **OK**.
- The link between the two selected devices will be displayed on the map.
- 

## Delete a Manually Added Link

Links that were added manually to the map can be deleted from the system.

- Manually added managed links are deleted from the Links table, as described in the procedure below.
- Manually added unmanaged links are deleted by clicking on the link in the map and then clicking **Delete** in the Link panel.

To delete a manually added managed link:

- 
- Step 1** In the left sidebar, choose **Inventory > Other > Links**.
- Step 2** Filter the Status column of the Links table to show Pre-provisioned links and select the required link.
- Step 3** Click the **Delete** icon to delete the link. The Delete icon is only enabled for manually added links.
- 

## Rename a Link

By default, the link name is generated automatically by the system based on the A- and Z-end interface name. You can rename any link, in which case the new name will represent the link in all link tables, in the Link 360 view, and on the map.

To rename a link:

- 
- Step 1** Go to any of the link tables.
- Step 2** Select the link you want to rename.
- Step 3** Choose **Actions > Rename**.
- Step 4** Enter a unique name for the link and click **Rename**.
- 

## Change Which Link and Device Types are Shown in the Network Topology Map

You can choose to display only certain types of links or devices in the network topology map. Click the **Show** button and select **Links** or **Device Families** to see a full list of link and device types and select the ones you want to display.




---

**Note** Link/device type filters are disabled when you select a specific circuit/VC to display on the map.

---

- 
- Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click on the **Device Groups** button, select the required device group(s), and click **Load**.
- Step 3** Click **Show** in the topology toolbar and choose **Links** or **Device Families**.
- Step 4** In the Links dialog:
- Select the types of links you want displayed in the topology map, for example, physical layer links, Ethernet layer links, and so on. The Links dialog only shows link types that exist in your network. If a link type exists in your network but not in the selected device group, it will be disabled.
  - If you want to differentiate aggregated links from single links, select the Display Aggregated Links as check box.
  - You can enable bandwidth utilization visualization on links that support this feature. See [Show Bandwidth Utilization for Links on the Map, on page 166](#) for more information.
  - Click **OK**. The topology map will reflect your selections. Only the link types you selected will be displayed.

**Step 5** In the Devices dialog:

- Select the device types you want displayed in the topology map, for example, routers, switches and hubs, optical networking, and so on. The Devices dialog only shows device types that exist in your network. If a device type exists in your network but not in the selected device group, it will be disabled.
- Click **OK**. The topology map will reflect your selections. Only the device types you selected will be displayed.

**Note** If you have selected to display optical networks on the map, by default you will see the devices that serve as optical line amplifiers (if any). Deselect the Display Optical Line Amplifier check box under Device Functions if you do not want these optical line amplifier devices to be displayed on the map.

## Show/Hide Alarms and Labels in the Topology Map

You can choose to hide the device name labels and you can hide alarms altogether or you can display alarms of specific severities only.

**Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.

**Step 2** Click the **Show** button in the topology toolbar.

**Step 3** Select the items you want displayed in the topology map:

- Labels—Labels associated with devices, such as device names.
- Faults—Deselect the check box to hide fault information altogether. Select the check box to show all alarms or use the slider to show only faults of a certain severity or higher.

**Step 4** Close the Show dialog. Your selections are applied to the topology map.

## Save Global Preferences for the Map Display

The **Show** button in the map toolbar allows you to choose the items that will be shown in your map display, including device names (labels), device types, link types, alarm severity, and so on.

If you are a Super User or Admin user, you can save your choices as global preferences which will be applied automatically for all new users and which can be loaded by any users on demand. You can also delete global preferences.

The following items are saved as global preferences:

- Labels on/off
- Device families
- Link types
- Fault severity
- Bandwidth utilization

To save global preferences for map display:

- 
- Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click on the **Device Groups** button, select the required device group(s) and click **Load**.
- Step 3** Click **Show** in the topology toolbar and select the items you want to show on the map.
- Step 4** Choose **Global Preferences > Save**.
- Saved global preferences can be deleted if necessary by clicking **Delete**.
- 

## Load Global Preferences for the Map Display

The **Show** button in the map toolbar allows you to choose the items that will be shown in your map display, including device names (labels), device types, link types, alarm severity, and so on.

If global preferences have been defined for the map display, you can load them. You can then make your own changes to the map display as required.

The following items are saved as global preferences:

- Labels on/off
- Device families
- Link types
- Fault severity
- Bandwidth utilization

To load global preferences for map display:

- 
- Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click on the **Device Groups** button, select the required device group(s) and click **Load**.
- Step 3** Choose **Global Preferences > Load**. This option is disabled if no global preferences have been defined.
- 

## Isolate Specific Sections of a Large Topology Map

In cases where a topology map is displaying thousands of devices, you might want to focus on specific devices or sets of devices. The Overview pane shows you the entire topology map in miniature and lets you select the area you want to display in the large topology map. It also provides an at-a-glance view of the alarm status of the elements in the topology map.

- 
- Step 1** Click the Overview icon in the topology toolbar. The Overview pane appears in the at the bottom right of the topology map and displays the following:
- Dot—indicates any network element. The color of the dot indicates the severity of alarms associated with the network element.
  - Line—indicates a link. The color of the line indicates the severity of the associated alarm.

- Blue rectangle—indicates the selection area. The area within the rectangle is displayed in the map pane. Handles on the corners enable you to resize the selection area.
- Pan mode cursor—cursor displayed within the selection area. Use this cursor to move the selection area, and thereby view different elements in the map pane.
- Zoom mode cursor—displayed outside the selection area. Use this cursor to define a new selection area or to zoom in on an existing selection area.

**Step 2** Draw a rectangle by dragging the mouse over the area you want to see in the topology map.

**Step 3** Click the 'x' in the upper right corner to close the Overview pane.

## Get More Information About Devices

From the topology map, you can drill down to get more information about a device.

**Step 1** Click on the required device in the topology map. A popup appears showing basic device information and alarm information for the device.

**Step 2** Click **View 360** to access the Device 360 view for detailed information about the device.

For more information, see, [Get Basic Device Information: Device 360 View, on page 63](#).

## Get More Information About Links

Cisco EPN Manager provides a variety of ways that you can view links and get more details about them:

To view link information for:	See the procedures in:
A specific link	<a href="#">Get a Quick Look at a Specific Link: Link 360 View, on page 160</a>
A specific link in a topology map	<a href="#">View a Specific Link in the Topology Map, on page 163</a>
A group in a topology map	<a href="#">View a Device Group's Links in a Network Topology Map, on page 163</a>
All of Cisco EPN Manager	<a href="#">View Link Tables , on page 164</a>

### Get a Quick Look at a Specific Link: Link 360 View


The Link 360 view gives you a quick look at the configuration and status of a device's links. Each Link 360 view provides information about the A- and Z-sides of the link (type, direction, capacity, and so forth). Depending on the link and device type, it also provides a wide range of metrics, such as power level, span loss, and bit errors.






You can launch the Link 360 view by clicking the "i" next to a link name in any of the link tables. This includes the tables that are opened by clicking **Links Table** in a topology map, or by choosing **Inventory > Other > Links**.

The Link 360 view provides general link and performance information at the top of the view, and more detailed link information in tabs in the lower part of the view.

Information Provided in Link 360 View	Description
General information	<p>The link name, serviceability status, highest severity alarm, type, direction, capacity, and utilization. Definitions of link serviceability states are provided in <a href="#">Link Serviceability States, on page 161</a>.</p> <p>If the link you are viewing is an OTS or OTU link, you can click the <b>Utilization</b> field's <i>i</i> (<b>information</b>) icon to open the <b>Used Wavelengths</b> pop-up window, which lists the optical channels configured on the link and the circuits that are currently using those channels.</p>
Performance data	Graphs or charts reflecting various aspects of link performance.
Alarms	Current alarms for the link, including their severity, status, the time they were generated, the source of the alarm, and the alarm's ID. Also provides a launch point for the Alarm Browser.
Links	(LAGs only) Status, name, and IP address for the A-side and Z-side port in the Link Aggregation Group.
Endpoints	<p>Devices and interfaces that serve as endpoints for the link. Provides a launch point for the Interface 360 view. For optical devices, this tab also displays the latest recorded power values for transmitted and received signals.</p> <p><b>Note</b> Power values are not normally displayed for manual links. However, if you open the Link 360 view for a manual LMP or OTS link between a Cisco NCS 1000 and 2000 device, the view displays the power values for both endpoints.</p>
Circuit/VCs	(For a circuit/VC that traverses the link) Circuit/VC name, type, customer, status, and creation date. Also provides a launch point for the Circuit/VC 360 view.
SRRGs	Lists the Shared Risk Resource Groups (SRRGs) assigned to the link or to the link endpoint devices. For each listed SRRG, you can see whether it is the default SRRG on the link/device or if it has been assigned to the link/device. For more information about SRRGs, see <a href="#">View and Manage Shared Risk Resource Groups (SRRG) in the Geo Map</a> .

## Link Serviceability States

Serviceability State	Icon	Description
Admin Down		Link was purposefully shut down by the administrator.

Down		Link is down (but it should not be).
Up		Link is up and traffic is passing through the link.
Auto Up		Link is up because it detected a signal (this state is only supported by optical devices).
Unavailable		Link is not discovered yet or its status is unavailable.
Partial		<p>Link has a mismatch between requests, resources, or resource states. Examples:</p> <ul style="list-style-type: none"> <li>• Link is processing a request to activate some service resources and deactivate others.</li> <li>• Link has some active and some deactivated resources.</li> <li>• Some link resources are up and others are down.</li> <li>• The state for one of the link's resources is not known.</li> </ul>

## Compare Link Information and Status

From the **Comparison View**, you can perform a side-by-side comparison of multiple links, viewing information such as raised alarms and the status of associated endpoints, circuits, and VCs. To compare links, do the following:

- 
- Step 1** For each link you want to compare:
- Open its **Link 360** view, as described in [Get a Quick Look at a Specific Link: Link 360 View](#).
  - Choose **Actions > Add to Compare**.
- The link you selected is displayed at the bottom of the page. You can select a maximum of 4 links.
- Step 2** Click **Compare**.
- The **Comparison View** opens.
- Step 3** From the drop-down list at the top of the view, specify whether the view will show all available information or just the information that is unique to each link.
- Step 4** Click **Comparison View**, check the check box for the categories you want the view to display, and then click **Save**.
- By default, all of the categories are already selected.
- Step 5** Scroll down the page to view the information provided for each category you selected.
- Note the following:
- The **Comparison View** only displays information for two links at a time. If you selected more than two, you will need to toggle to the links that are not currently displayed.
  - To reorder the links you have selected, click **Rearrange**.
  - Each link's **Actions** menu is identical to the one provided in its **Link 360** view. If you select an option, the corresponding page opens.



- You can minimize and maximize the categories displayed, as needed.
- The **Comparison View** is also available for circuits and VCs, devices, and interfaces. Whenever you select any of these elements from their respective 360 view for comparison, they are displayed in the corresponding tab. This allows you to switch between element types, as needed.
- When you are done comparing links, click **Back** at the top of the view and then click **Clear All** at bottom of the page. If tabs for other element types are still displayed, you will need to clear them as well.

---

## View a Specific Link in the Topology Map

You can select a specific link from the following pages and view the link in the topology map:

- Launch the Link 360 view, and then choose **Actions > Show in Topology**. For information about how to launch the Link 360 view, see [Get a Quick Look at a Specific Link: Link 360 View, on page 160](#).
- From the links table, select a specific link, and then choose **Actions > Show in Topology**. You can access the links table by clicking the Links Table hyperlink under the Links tab in the topology map, or by choosing **Inventory > Other > Links**.

## View a Device Group's Links in a Network Topology Map

Cisco EPN Manager uses the following conventions to represent links in the topology map:

- A solid line represents any type of discovered link between two elements in the topology map.
- A dotted line represents an unmanaged link that was manually drawn in the topology.
- (If enabled in the **Show > Links** menu) A dot-dash line represents an aggregated link.
- If there is a critical alarm on a link, the link will be colored red and the alarm icon will be displayed on the link.
- If an existing link is down and there is no critical alarm on the link, the link will be colored grey and a "?" icon will be displayed on the link. After 6 hours, the link will be removed automatically from the map but it can be deleted manually from the Links table or from the Link details view before that time if necessary.

If an alarm severity badge is displayed on a link, it represents the most severe alarm that is affecting the link. For aggregated links, it represents the most severe alarm affecting any of the links in the aggregation.

To get more information about links in a topology map:

- Hover over the link with your mouse to display a panel that provides "at-a-glance" useful information about that link, such as the most severe alarms, or bandwidth utilization information for the link, if available. If there are no alarms on the link and there is no bandwidth utilization information, this panel will not be displayed. If there are alarms on the link, you can click the number next to the alarm severity icon to display a table listing only those alarms.
- Click on a link to display a popup window with link information, including link type, the link's A- and Z-side devices and interfaces, and link utilization. For aggregated links, the popup window lists all the underlying links, as in the following example:

**Link Details**  
ASR903-AGN-1.cisco - ASR903-PAN-6

Type Aggregated (2)

	Alarm	Name	Type	A End Device	A End Interface	A End Utilization	Z End Device	Z End Interface	Z End Utilization
		LDP 8.8.8.8...	LDP	ASR903-...	ASR90...		ASR903-P...	ASR90...	
		LINK PW ...	Pseu...	ASR903-...	PW 8.8...		ASR903-P...	PW 16...	

## View Link Tables

Cisco EPN Manager provides a table that lists all of the links that it is managing. This provides a quick way to locate all links of a specific type or with a name that shares a common string. You can also identify links that have severe alarms, and launch Interface 360 views for view the affected sides.

The table also provides a quick look at link utilization and capacity.

In addition, you can open a table showing links for the current group being displayed in the topology map. This table provides the same information and actions as the table of all links in the system.

### Step 1 To display link tables:

- For all links: In the left sidebar, choose **Inventory > Other > Links**.
- For a selected device group's links: In the left pane of the topology map window, select the Links tab, then click the **Detach** icon in the top right corner or click the Links Table hyperlink at the bottom of the tab. The Links table is displayed in a separate window.

### Step 2 From here you can do the following:

- Find specific types of links—for example, Physical, Pseudowire, LAG, ODU, and so forth. Place your mouse cursor in the Type field and select the link type from the drop-down list. You can also find Manual Links in this manner.
- Find links by name by entering text in the Link Name text box. You can also enter a partial string (for example, 3.3.3.3\_).
- Find links with severe alarms by clicking in the Severity text box to display a severity drop-down list, then choosing a severity. You can perform this same procedure from the A-side or Z-side. The table will indicate which side of the link has the more severe alarm, and you can launch an Interface 360 view for both sides.
- See the operational and discovery status of links in the Status column. Links can have an operational status of Up or Down. The discovery status can be one of the following:
  - Pre-provisioned: Managed links that were created manually by a user and were not discovered by the system. These links can be deleted from the system and from the map. Select the link and click the Delete icon.
  - Pre-provisioned-Incomplete: Manually created links that could not be fully discovered.
  - Discovered-Incomplete: Links that could not be fully discovered. These partially discovered links are not shown on the topology map.

- **Unknown:** Existing links that are down and therefore can no longer be discovered. These links remain on the topology map for 6 hours but they are colored grey and are identified by an "?" icon on the link. Links with Unknown status can be deleted by selecting the link in the table and clicking the **Delete** button.
- See bandwidth utilization for optical (OTS, OTN, ODU), packet (physical, LAG), and cable (L2TP) links. The Utilization column for each side of the link shows the actual usage data (for example, number of channels for OTS links), the percentage of total capacity used, and the default time period for which utilization is calculated (1 hour). The Capacity column shows the total bandwidth capacity of the link.

**Note** To show utilization for packet and cable links, an Interface Health monitoring policy must be created and enabled on the relevant devices. See [Set Up Basic Interface Monitoring, on page 195](#) for more information.

Type	A End ...	A End	A End Utilization	Z End ...	Z End	Z End Utilization	C
Physical	Critical	GigabitEth...	0% (1.2800899e-7 Gbps) 1h	Clea...	GigabitEth...	0% (3.8312794e-7 Gbp:	1 C
Physical	Clea...	GigabitEth...	0% (1.574779e-7 Gbps) 1h	Clea...	GigabitEth...	0% (4.6376692e-7 Gbp:	1 C
Physical	Clea...	TenGigabi...	0% (0.000044290136 Gbps) 1	Clea...	TenGigabi...	0% (0.00003339692 Gb	10
Physical	Clea...	TenGigabi...	0% (0.000071106515 Gbps) 1	Clea...	TenGigabi...	0% (0.00007004112 Gb	10
Physical	Clea...	GigabitEth...	0% (3.2127232e-8 Gbps) 1h	Clea...	GigabitEth...	0% (0.0000010210271	1 C
Physical	Clea...	GigabitEth...	0% (6.619419e-8 Gbps) 1h	Clea...	GigabitEth...	0% (1.9693468e-7 Gbp:	1 C
Physical	Clea...	TenGigabi...	0.03% (0.002898862 Gbps) 1h	Clea...	TenGigabi...	0.03% (0.0028905713 C	10
Physical	Clea...	GigabitEth...	0.05% (0.00047108906 Gbps)	Clea...	GigabitEth...	8.01% (0.08006172 Gb	1 C
Physical	Clea...	GigabitEth...	0% (8.722009e-8 Gbps) 1h	Clea...	GigabitEth...	0% (6.596751e-8 Gbps	1 C
Physical	Clea...	GigabitEth...	0% (8.718443e-8 Gbps) 1h	Clea...	GigabitEth...	0% (6.419498e-8 Gbps	1 C
Physical	Clea...	TenGigabi...	1.25% (0.12529424 Gbps) 1h	Clea...	TenGigabi...	1.09% (0.109484255 G	10
Physical	Clea...	GigabitEth...	0.03% (0.00029982472 Gbps)	Clea...	GigabitEth...	26.69% (0.2668724 Gb	1 C
Physical	Clea...	TenGigabi...	0.03% (0.0028978328 Gbps)	Clea...	TenGigabi...	0.03% (0.0028960628 C	10
LAG	Clea...	ASR-9K-...	17.35% (0.34694874 Gbps) 1h	Clea...	ASR920_...	0.04% (0.00077091146	2 C
Physical	Clea...	TenGigabi...	1.1% (0.109563656 Gbps) 1h	Clea...	TenGigabi...	1.24% (0.1243847 Gbp:	10

- Depending on the link type, perform an action by choosing a link and making a selection from the **Actions** drop-down menu. (For example, for OTS links, you can run an OTDR Scan).
- View a specific link on the topology map by clicking **Actions > Network Topology**.

## Troubleshoot Link Issues

This section presents suggested solutions for issues you might encounter when working with links.

Link Issue	Possible Cause	Solution
Links that previously existed disappear from the topology map.	The hostname might have been changed on one of the endpoint devices.	<ol style="list-style-type: none"> <li>1. Delete the device on which the hostname was changed from the system and then add it again.</li> <li>2. Sync the device and all devices connected to it to make sure that all information is updated.</li> </ol>

## Show Bandwidth Utilization for Links on the Map

In the topology map and in the geo map, you can enable visualization of the bandwidth utilization for optical links (OTS, OTN, and ODU), packet links (physical and LAG), and cable links (L2TP) over which circuits are provisioned. In this way, you can easily identify when a link is over-utilized or approaching over-utilization. Bandwidth utilization is supported for one link type at a time. Click on the **Utilization** button in the top right corner of the topology map or the geo map to enable/disable visualization of bandwidth utilization and to select the link type to be displayed.



### Note

To show utilization for packet and cable links, an Interface Health monitoring policy must be created and enabled on the relevant devices. See [Set Up Basic Interface Monitoring, on page 195](#) for more information.

When bandwidth utilization is enabled for a specific link type:

- A thicker link is shown in the map and is colored based on the percentage of total bandwidth currently being used by provisioned circuits on the link. Click the "i" icon in the Utilization panel at the top right of the map to see the color representations for the bandwidth utilization. The thresholds for bandwidth utilization coloring can be set up in Administration > Settings > System Settings > Maps > Bandwidth Utilization. See [Define Color Thresholds for Link Bandwidth Utilization](#)
- Bandwidth utilization data is provided in all link-related views, for example, the Link panel that is displayed when you click on a link, Links tables, the Link 360, and so on.

Bandwidth utilization is calculated as follows:

- For OTS links between NCS 2000 devices, link capacity is calculated from the fiber-attributes parameters configurable on the devices. If OTS links are configured to allow SSON circuits (channel number is set to "Nyquist"), capacity is assumed to be 96 channels. Bandwidth utilization is calculated in terms of the number of 50Ghz ITU channels used in relation to the capacity. For SSON circuits the result is approximated because each Carrier NC or Carrier Trail counts as one channel used, regardless of its actual size.

Click on the **i** icon in the Utilization column to display a dialog showing details of exactly which channels are being used and which circuits are using the channels.



---

**Note** The dialog shows only 50 GHz ITU wavelengths/frequencies, therefore SSON carrier circuits might not be shown.

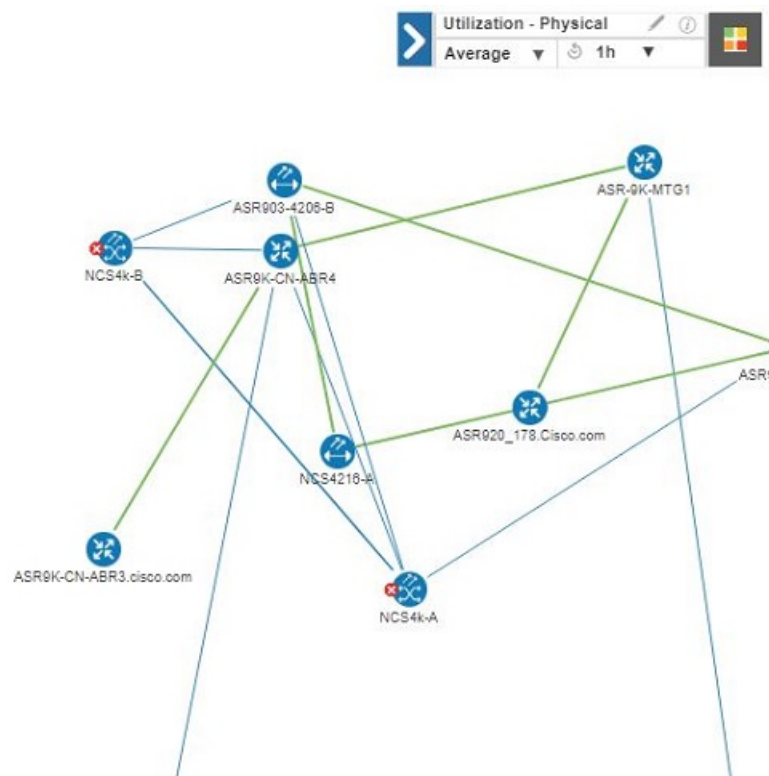
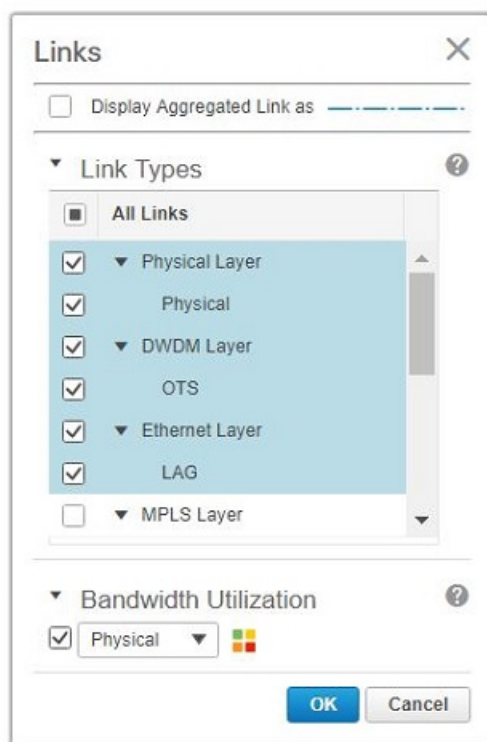
---

- For OTN and ODU links, bandwidth utilization is calculated based on the number of ODU0 timeslots reserved and is represented in gigabits per second.
- For physical and LAG links, bandwidth utilization is calculated from the input and output data rate of the link interfaces. For these link types you can define whether you want to see the average utilization or the peak utilization. You can also specify the time period for which you want to show utilization data - 15 minutes, 1 hour, 6 hours, or 1 day.
- For cable L2TP links, L2TP utilization is calculated for available L2TP tunnels. If L2TP tunnels are present then L2TP link utilization is calculated per RPD by getting the OFDM channels utilization of the associated downstream controller.

To enable visualization of bandwidth utilization:

- 
- Step 1** Open the topology map.
  - Step 2** Click on the **Device Groups** button, select the required device group(s), and click **Load**.
  - Step 3** In the top right corner of the topology map, click the **Utilization** button.
  - Step 4** In the displayed Links dialog, select the **Bandwidth Utilization** check box and select the required link type. Note that bandwidth utilization will be disabled if there are no supported link types in the map for the selected device group.
  - Step 5** Click **OK**.
- 

In the topology map, the links of the selected type will appear thicker and will be colored based on the bandwidth utilization of the link.



## Define Color Thresholds for Link Bandwidth Utilization

When bandwidth utilization visualization is enabled, links in the map are colored based on the percentage of total bandwidth currently utilized on the link. See [Show Bandwidth Utilization for Links on the Map, on page 166](#). Default thresholds are defined by the system, however, you can define your own thresholds to determine how bandwidth utilization will be reflected on the links.

To define color thresholds:

- 
- Step 1** Select **Administration > Settings > System Settings > Maps > Bandwidth Utilization**.
- Step 2** Select the type of link for which you are defining thresholds.
- Step 3** In the Link Coloring Thresholds area, define the criteria for coloring the links. Each row defines a color and the bandwidth percentage range that the color will represent. The default thresholds are: Green - 0-25%, Yellow - 26-50%, Orange - 51-75%, and Red - 76-100%. You can edit each row and/or you can add or delete rows using the plus and minus buttons.
- Note the following:
- A maximum of 10 thresholds can be defined.
  - The first threshold must start from zero and the last threshold must end with 100.
  - The thresholds must be sequential, meaning that each row's range must follow on from the previous row's range. For example, if the range in row 1 is 0-25%, row 2's range must start with 26%.

**Step 4** Click **Save**.

If you enable bandwidth utilization visualization in your map, the links will be colored according to these thresholds.

## View Fault Information for Devices and Links

If a device or link has an alarm associated with it, an alarm badge is displayed on the device icon or on the link in the topology map. The color of the alarm badge corresponds with the alarm severity—minor (yellow), major (orange), or critical (red)—and matches the alarms displayed in the Alarm Browser.

For groups, the alarm badge represents the most severe alarm that is currently active for any of the group members.

Link-related alarms, such as Link Down, generate an alarm badge on the relevant link in the topology map. After the link up alarm is received, the link alarms and corresponding badges are cleared.

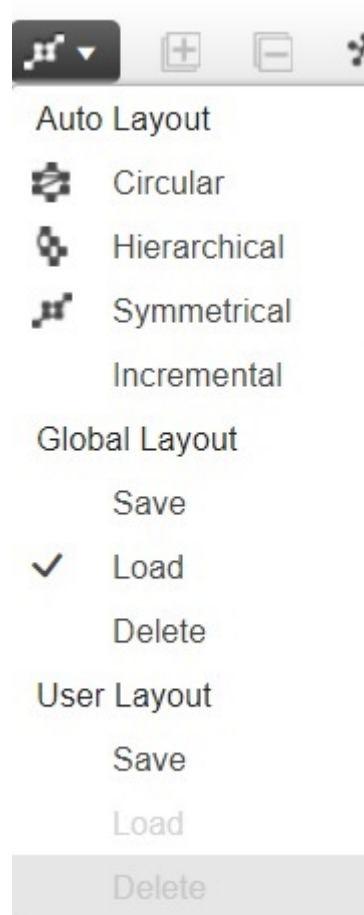
See [Alarm Severity Icons, on page 221](#) for more information.

## Change the Layout of a Network Topology Map

When you first open the topology map, it is displayed according to the default global layout. The global layout can be changed by users with network topology "edit" privileges. Any changes you make in the map are maintained for the current browser session only, meaning that when you next open the map, the global layout will be applied. If you want your own map layout to be preserved for future sessions, you can save your layout. Your saved layout overrides the global layout.

Click the **Layout** icon in the topology toolbar to access the layout options.





- A checkmark indicates which layout is currently being used. For example, a checkmark next to "Load" under Global Layout indicates that the global layout is currently being used.
- If you move devices around in the map and you want to save the new layout as the global layout for all users, click **Save** under **Global Layout**. This option is only available for users with network topology "edit" privileges.
- If you move devices around in the map and you want to save your own layout for the next browser session, click **Save** under **User Layout**.
- If the global layout is being used and you want to use your own saved layout, click **Load** under **User Layout**.

You can specify how the devices and other network elements (such as labels, nodes, and the connections between them) are arranged in the topology map by dragging them to the required position in the map or by selecting one of the predefined options:

- Symmetrical (default)—Maintains the symmetry that is inherent in the topology. This ensures that adjacent nodes are closer to each other and prevents node overlapping.
- Circular—Arranges the network elements in a circular style highlighting the clusters inherent in the network topology.



- Hierarchical—Ensures that the dependencies on the relationships and flows between elements are maintained.
- Incremental—Maintains the relative positions of specific elements while adjusting the positions of newly added elements. Use this layout to re-render nodes/links and to clean up overlaps.

## Add a Background Image to the Network Topology

A background image can be applied to the topology map for any selected group. This is useful if, for example, you want to group your network according to geographic location. A sub-group can have a different image from its parent group. For example, you could apply a country map to one group and state maps to its sub-groups. Background images are saved per group and per user.

When a background image is applied, zoom functionality is supported and devices maintain their location on the image as you zoom in and zoom out.

The system provides some predefined images that you can select as background images. Alternatively, you can use your own custom background images.

### Before you begin

When adding a custom background image, follow these guidelines:

- The background image file must reside on the server in a directory that is covered by high availability (HA), meaning that it will be moved to the secondary server in the case of primary server failure.
- Images should be in .png or .jpg format (.png is recommended).
- The file size should be as small as possible because the time taken to render the map is directly proportional to the size of the image.

- 
- |               |                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the left sidebar, choose <b>Maps &gt; Topology Maps &gt; Network Topology</b> .                                                                          |
| <b>Step 2</b> | In the Network Topology window, click the <b>Add Background Image</b> icon in the topology toolbar. The Manage Group Background Image dialog opens.         |
| <b>Step 3</b> | Choose the required group from the Select Group drop-down list.                                                                                             |
| <b>Step 4</b> | Choose <b>Predefined</b> or <b>Custom Image</b> from the Background Image drop-down list.                                                                   |
| <b>Step 5</b> | For a custom image, click <b>Select Image</b> , navigate to the image file and double-click it. For a predefined image, select one of the displayed images. |
| <b>Step 6</b> | Click <b>Apply</b> .                                                                                                                                        |
| <b>Step 7</b> | In the topology map, arrange the devices as required (devices are arranged randomly on the map).                                                            |
| <b>Step 8</b> | Save the new layout by choosing <b>Layout &gt; Save Current Layout</b> .                                                                                    |
- 

## Visualize and Trace Circuits/VCs

When working with circuits/VCs, it is very useful to see how a circuit/VC is deployed within the existing network topology. Cisco EPN Manager overlays the circuit/VC on an existing topology map, clearly indicating the endpoints and midpoints of the circuit/VC, the role of the endpoint (where relevant), and relevant fault information for the circuit/VC. If the selected group does not contain all the devices participating in the

circuit/VC, a popup is displayed asking if you want to switch groups to show the full overlay. See [View and Manage Discovered/Provisioned Circuits/VCs, on page 519](#) for more information.

## Display Routes of a Circuit

For optical and CEM circuits, you can display routes associated with a specific circuit.

To do this use the **Routes** drop-down menu in the topology toolbar. The Routes menu calculates the routes from the links within a service. You can also see more data about the circuit routes. For example, the working path is represented with a 'W' label and the Protected path with a 'P' label on the links. See [Display the Routes Associated With a Circuit, on page 539](#).

## Trace and Visualize the Full Route of a Circuit

You can do a full multi-layer trace of a circuit from the Network Topology window. See [Trace and Visualize the Full Route of Circuits/VCs, on page 568](#) for more information.

## Show Clock Synchronization Networks on a Network Topology Map

If Synchronous Ethernet (Sync-E) or Precision Time Protocol (PTP) clock synchronization is configured on the devices in your network, you can visualize the clock synchronization network on the topology map.

- The Sync-E overlay shows the topology and hierarchy of the sync-E network, including the primary clock and the primary and secondary clock inputs for each device. This allows the clock signal to be traced from any Sync-E enabled device to the primary clock or from the primary clock to a Sync-E enabled device.
- The PTP overlay shows the clock synchronization tree topology, the PTP hierarchy, and the clock role of each device in the tree - master, boundary, slave, or transparent.

---

**Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.

**Step 2** Click on the **Device Groups** button, select the required device group(s), and click **Load**.

**Step 3** Click **Show** in the topology toolbar and choose **Technology**. Click the question mark icon for a description of what will be displayed on the map for each technology.

**Step 4** Select the required technology and click **OK**.

The clock synchronization network is shown as an overlay over the existing network in the map. The legend at the bottom right explains the notations used in the map for the selected technology.

**Note** If you select a different device group, the technology overlay will be removed.

---

# Show Routing Networks on the Topology Map

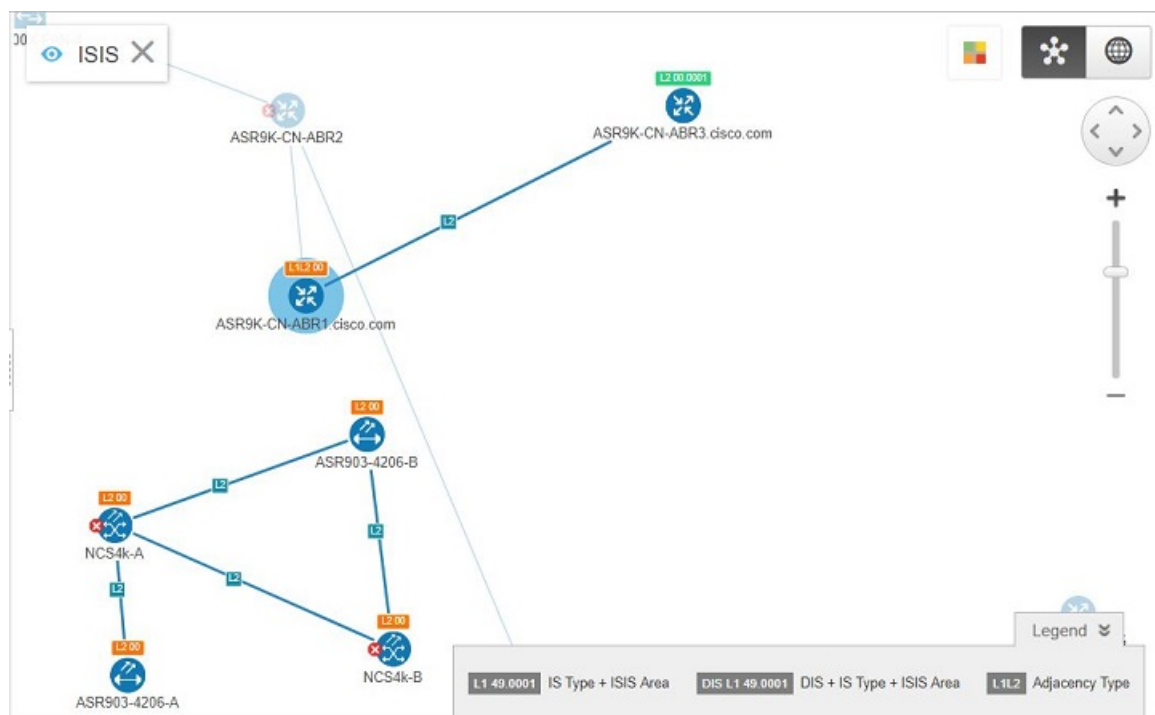
Routing protocols used in your network can be graphically represented as an overlay on the topology map. Overlay of the following routing protocols is supported:

- **OSPF:**
  - The OSPF overlay shows the different OSPF domains in the network and the links between them, which are labeled as inter-area OSPF links. The overlay shows the OSPF area ID to which each link belongs and the role of each router, for example, Area Border Router (ABR), Designated Router (DR), and so on.
  - OSPF overlay is supported on devices running IOS-XE (ASR 90x, ASR 920, and NCS 42xx devices) as well as devices running IOS-XR (ASR 9000, NCS 4000 devices). OSPF overlay is also supported on XR-XE cross-platform devices.
- **BGP:**
  - The BGP overlay labels each device with the ID of the autonomous system to which it belongs and shows the links within and between autonomous systems.
  - If two connected routers belong to the same autonomous system, the link is an internal BGP link. If they belong to different autonomous systems, the link is marked as an external link.
  - Each unique autonomous system has a different color so that you can easily identify devices belonging to the same AS.
  - The overlay also marks the devices that serve as route reflectors or route clients.
  - BGP overlay is supported on ASR 920, ASR 901, and ASR 901\_10G devices.
- **ISIS:**
  - The ISIS overlay shows the devices (Intermediate Systems - IS) running ISIS as the Interior Gateway Protocol (IGP). Above these devices, you will see a notation that indicates the IS type, the area ID which identifies the different ISIS domains, and an indication if the device is a Designated Intermediate System (DIS). The notation shows the first 6 bytes of the NET address. Hovering over the notation displays a tooltip containing the complete NET address and the process ID.
  - The IS type can be L1 for intra-area routing, L2 for routing between areas, or L1L2 for both intra- and inter-area routing.
  - Each ISIS domain is represented in a different color.
  - A notation on the links in the ISIS network indicates the ISIS adjacency. For aggregated links where multiple adjacency types exist, multiple adjacency type notations will be shown on the link.
  - ISIS overlay is supported on devices running IOS-XE (ASR 903, ASR 907, and NCS 42xx devices) as well as devices running IOS-XR (ASR 9000, NCS 4000 devices).



**Note** DIS indication is presented on the device level and not in the context of a specific IS level.

Following is an example of an ISIS overlay in the map:



To show a technology overlay in the map:

- Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click on the **Device Groups** button, select the required device group(s), and click **Load**.
- Step 3** Click **Show** in the topology toolbar and choose **Links**. Make sure that the map is showing the relevant types of link, for example, ISIS links, BGP links. In addition, if Bandwidth Utilization is enabled, disable it.
- Step 4** Click **Show** in the topology toolbar and choose **Technology**. Click the question mark icon for a description of what will be displayed on the map for each technology.
- Step 5** Select the required routing protocol and click **OK**.

The routing network is shown as an overlay over the existing network in the map. The legend at the bottom right explains the notations used in the map for the selected technology.

**Note** If you select a different device group, the technology overlay will be removed.

## Save the Topology Map as an Image File

You can save the entire topology map or selected objects from the topology map as an image file. This will enable you to store copies of the topology map in a specific state which you can use as a point of reference in the future when multiple changes are made to the topology.

To save the topology map as an image file:

- 
- Step 1** Choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click on the **Device Groups** button, select the required device group(s), and click **Load**.
- Step 3** Make content and layout changes to the topology map as required.
- Step 4** Click the Save Image icon in the topology toolbar.
- Step 5** In the Save As Image dialog box, select the file type for the saved image.
- Step 6** Choose whether you want to save the entire topology or only the items currently selected in the topology map.
- Step 7** Choose a size setting for the image file.
- Step 8** Click **OK**. The image is saved in your local Temp folder.
- 

## View Your Network on a Geographical Map (Geo Map)

- [Geo Map Overview, on page 175](#)
- [Geo Map Setup, on page 177](#)
- [Identify Which Devices are not Showing on the Geo Map \(Unmapped Devices\), on page 177](#)
- [Place Unmapped Devices on the Geo Map, on page 178](#)
- [Change the Location of a Device on the Geo Map, on page 178](#)
- [Change the Location of a Device in a Cluster, on page 179](#)
- [Remove a Device from the Geo Map, on page 179](#)
- [Identify Which Devices are not Showing on the Geo Map \(Unmapped Devices\), on page 177](#)
- [Search for a Device in the Map, on page 153](#)
- [View Link Layers in the Geo Map, on page 181](#)

## Geo Map Overview

The geo map enables you to position your network devices on a world map and monitor them within their geographical context. The displayed world map is either imported by accessing the map provider's site over the Internet (online mode) or from locally installed map resources (offline mode).



**Note** When working with the geo map in online mode, a connection to the Internet is required from each client or from the Cisco EPN Manager server if it is being used as a proxy.

The geo map is accessed via the topology map. To open the geo map:

- 
- Step 1** In the left sidebar, select **Maps > Topology Maps > Network Topology**
- Step 2** Click on the Geographical Map toggle button in the top right corner of the map.



About the geo map:

- You can switch back and forth between the topology map and the geo map using the toggle buttons in the top right corner of the map.
- The geo map displays devices for which GPS coordinates have been defined. Devices that do not have GPS coordinates do not appear on the geo map and are called “unmapped devices.” See [Place Unmapped Devices on the Geo Map, on page 178](#).
- You can click on a device in the geo map to see alarms, basic information, location coordinates and civic location (if it has been defined for the device).
- For optical devices that support GPS location configuration (NCS 2000 devices), any change that is made to the device's location in the geo map is synched with the device and vice versa (location changes made on the device itself will be reflected in the geo map).
- GPS coordinates are shown in DMM format (degrees and decimal minutes) but users can define GPS coordinates in DMM, DD (Decimal Degrees), or DMS (Degrees, Minutes, and Seconds) formats.
- If there are no devices on the geo map, the full world map is shown. If there are devices in a specific area, only that area of the world will be shown. The geo map shows only the portion of the world map that contains devices.
- As in the topology map, the geo map shows the devices in the selected device group. The device group selection is synchronized between the topology map and the geo map such that if you change the selection in one map, it will change in the other map as well.
- If there is a device group that has a defined geographical location within the selected device group it will be represented in the geo map with a device group icon. If the device group does not have a geographical location, its contained devices will be shown individually in the geo map. See [Device Groups in the Geo Map, on page 176](#) for more information.
- The geo map groups devices that are close to one another geographically in clusters, represented by a cluster icon with a number indicating the number of devices in the cluster. Zoom in to see the individual devices. See [Identify the Members of a Cluster, on page 180](#).
- As in the topology map, you can show a circuit/VC in the geo map. However, when initiating provisioning actions such as creating a circuit/VC or modifying a circuit/VC, the view will switch to the topology map.

## Device Groups in the Geo Map

In addition to individual devices, the geo map shows device groups that have a defined location, for example, devices in a building at a specific address.

Take the following into consideration when viewing groups in the geo map:

- Only location-type device groups can be shown in the geo map, and they are only visible if they have a defined geographical location. The location is defined in the device group properties. To create or edit a location device group and define the geographical location of the group, go to **Inventory > Group Management > Network Device Groups**. See [Create Location Groups, on page 60](#) for more information.
- Group members inherit the location of the group.
- If a group's location is the same as other devices/groups, it will be included in a cluster. The number displayed on the cluster icon represents the total number of devices in the cluster (including devices contained in groups).
- If there are alarms on any of the devices within a group, the highest severity alarm icon will be displayed on the device group icon.

- Click on the location group icon to see a panel containing information about the group, including its name, GPS coordinates, and alarm information. If civic location information is defined for the group, it will also be shown in this panel. Click on the **Show Members** link in the panel to show a list of the devices and sub-groups that belong to the group. Alternatively, double-click on the location group icon to achieve the same results.
- If a group member device is given a geographical location, the device will be shown on the geo map as an individual device and alarms will be shown on the device itself, not on the group. It is preferable to have all devices in a geographical location group inherit the GPS coordinates of the group in order to retain the significance of the group's location.

## Geo Map Setup

The system is set up by default to get the map tiles from a specific Mapbox URL through a direct Internet connection from the client or via the EPN Manager server which acts as a proxy. If required, you can use a different map tiles provider by providing a specific URL. Both of these options require an Internet connection. If you do not have an Internet connection, you can install the map resources locally and specify that you want the system to use the local map resources, which means that you are effectively working in offline mode.

The geo map setup can be managed in the System Settings. In the left navigation pane, select **Administration > Settings > System Settings > Maps > Network Topology**.

In the Network Topology page, you can do the following:

- Enable/disable the geo map. By default, geo map is enabled, meaning that all clients will have the geo map functionality. You can deselect the **Enable geo map** checkbox to disable the functionality.
- Identify the source for the map tiles (using an Internet connection). The default map tiles provider is Mapbox. If you are working with another map tiles provider, you need to provide the URL for map tiles access. Be sure to request the exact format of this URL from the map tiles provider. Select **Custom** in the Map Provider dropdown list and enter the URL. Note that the geo map functionality has not been tested with map tiles from providers other than Mapbox.
- Make the Cisco EPN Manager server a proxy for accessing the Internet to retrieve the map tiles. For security reasons, you might not want direct Internet access from each client. If you enable the **Via management application proxy** check box, Internet access to the map provider URL is via the Cisco EPN Manager server, not directly via the clients.
- Specify that you want to display the geo map using installed map resources that do not require a connection to the Internet. Select **Installed Map Resources** in the Map Provider dropdown list. Refer to the [Cisco Evolved Programmable Network Manager Installation Guide](#) for instructions on how to install the map resources.

## Identify Which Devices are not Showing on the Geo Map (Unmapped Devices)

For any selected device group, only the devices that are defined with GPS coordinates will automatically be shown on the geo map. When you switch to the geo map or when you select a different device group, a popup message will indicate how many unmapped devices there are, meaning how many devices that do not have coordinates and therefore do not appear on the map.

To identify which devices are not being shown on the geo map, click the **Unmapped Devices** button above the map.

## Place Unmapped Devices on the Geo Map

You can either drag and drop unmapped devices onto the required location on the geo map or you can specify the GPS coordinates to define the device's location on the geo map.

GPS coordinates can be specified in any of the following formats:

- Degrees and decimal minutes (DMM): 41 24.2028, 2 10.4418
- Decimal degrees (DD): 41.40338, 2.17403
- Degrees, minutes, and seconds (DMS): 41°24'12.2"N 2°10'26.5"E



**Note** When using DMS format, please use a double quotation mark (") to indicate the seconds.

To place unmapped devices on the geo map:

- 
- Step 1** In the left sidebar, select **Maps > Topology Maps > Network Topology**
- Step 2** Click on the Geographical Map toggle button in the top right corner of the map.
- Step 3** Click the Unmapped Devices button above the map.
- Step 4** In the Unmapped Devices panel on the right, either:
- Drag and drop a device onto the map or select multiple devices and drag and drop them onto the map.
  - Select the device(s) you want to place on the map and click **Set Location**. In the displayed dialog, specify the GPS coordinates, for example, Latitude 59.623325, Longitude-103.535156. Click **Place Device**.
- Note** If you select multiple devices, they will be consolidated into a cluster and placed on the same location on the map. The cluster icon indicates how many devices the cluster contains.
- 

## Change the Location of a Device on the Geo Map

To move a device to a different location on the geo map, you need to open the Edit Location dialog and then either drag the device to the required location on the map or set the coordinates manually. If the device is in a cluster, you must open the cluster to view the devices and then change the location of the device.

GPS coordinates can be specified in any of the following formats:

- Degrees and decimal minutes (DMM): 41 24.2028, 2 10.4418
- Decimal degrees (DD): 41.40338, 2.17403
- Degrees, minutes, and seconds (DMS): 41°24'12.2"N 2°10'26.5"E



**Note** When using DMS format, please use a double quotation mark (") to indicate the seconds.

To change the location of a device:



- 
- Step 1** Click on the device on the geo map. A popup appears showing basic device information and alarm information for the device.
  - Step 2** Click **Edit Location**. The Edit Location dialog opens.
  - Step 3** Drag the device to the required location or change the GPS coordinates as required.
  - Step 4** Click **Save**.
- 

## Change the Location of a Device in a Cluster

Devices that are very close to each other in location are grouped in a cluster on the geo map. You can change the location of one or more of the devices in the cluster. The device will be removed from the cluster and will appear on the geo map as an individual device.

To change the location of a device in a cluster:

- 
- Step 1** Click on the cluster in the geo map. A popup appears showing basic information for the cluster.
  - Step 2** Click **Show Devices**. A panel is displayed to the right of the map and lists all the devices in the cluster.
  - Step 3** In the panel on the right, either:
    - a) Drag and drop a device onto the map or select multiple devices and drag and drop them onto the map.
    - b) Select the device(s) you want to place on the map and click **Set Location**. In the displayed dialog, specify the GPS coordinates, for example, Latitude 59.623325, Longitude-103.535156. Click **Place Device**.The device(s) will be removed from the cluster and placed in the specified location on the map.
- 

## Remove a Device from the Geo Map

If you no longer want to display a device on the geo map, you can remove it. The removed device will appear in the Unmapped Devices list.

To remove a device from the geo map:

- 
- Step 1** Click on the device on the geo map. A popup appears showing basic device information and alarm information for the device.
  - Step 2** Click **Edit Location**.
  - Step 3** In the Edit Location dialog, click **Remove Location**.
- 

## Remove a Clustered Device from the Geo Map

Devices within clusters can be removed from the geo map. You can remove an individual clustered device or you can remove multiple devices in the same cluster at one time. The removed device(s) will appear in the Unmapped Devices list.

To remove clustered devices from the geo map:

- 
- Step 1** Click on the cluster containing the device(s) you want to remove. A popup appears showing basic device information and alarm information for the device.
  - Step 2** Click **Show Devices**. A list of the devices contained in the cluster is displayed.
  - Step 3** Select the device(s) you want to remove.
  - Step 4** Click **Set Location**.
  - Step 5** In the displayed dialog, click **Remove Location**.
  - Step 6** Click **Yes** in the warning message informing you that the devices will be moved to the Unmapped Devices list.
- 

## Identify the Members of a Cluster

A cluster is formed when two or more devices or device groups are located close to one another on the map. The cluster is represented on the geo map by a circle with a number in its center, indicating the number of devices in the cluster (including individual devices and devices within groups). Zoom in to see the individual cluster members on the map.




---

**Note** If cluster members are very close to each other (approximately 8 meters apart or less), zooming in will not show the individual devices/groups. Follow the procedure below to see the individual members of the cluster.

---

To see a list of the devices/groups in a cluster:

- 
- Step 1** Click on the cluster icon.
  - Step 2** In the displayed popup, click **Show Members**. The devices or device groups contained in the cluster are listed in the panel to the right of the map. If the cluster contains groups, you can drill down to see the devices in the group. Use the navigation links at the top of the dialog to return to the previous list.
  - Step 3** You can change the location of a device by dragging it from the list onto the map or by clicking **Set Manually** and specifying new coordinates.
- 

## Search for a Specific Location in the Geo Map

You can search for a specific location in the geo map, for example, a state, country, town, or a specific address. If you enter a keyword in the search box, the results will show all locations that contain that keyword, down to the level of a specific street. You can then select the required location in the search results to pinpoint it in the map.




---

**Note** Internet connectivity is required to perform this location search.

---

To search for a specific location in the geo map:

- 
- Step 1** Click the **Search** icon in the toolbar.
- Step 2** Type the full or partial result in the search text box and press **Enter**.  
The Address tab in the search results panel lists locations that match your search.
- Step 3** Select a location in the search results.  
The map pans and zooms to the specified location and a marker on the map indicates the exact location.
- 

## View Link Layers in the Geo Map

In the geo map, you can see a three-dimensional view of the links in your network, separated by link type.

Click the Link Layers icon on the right to access the 3D link layers view. Click the icon again to return to the full geo map.

The 3D link layers view consists of up to three separate layers. The lower layer shows the geo map with all its links and devices. The two upper layers show links of a specific link type category (e.g., physical layer, control plane, and so on), together with the relevant devices. The layers shown in the 3D link layers view correspond with the link type categories currently selected for display in the link filter (click the Filter icon in the toolbar and select Link Types).



---

**Note** Several operations such as pan, zoom, filter, and search are not available in the 3D link layers view.

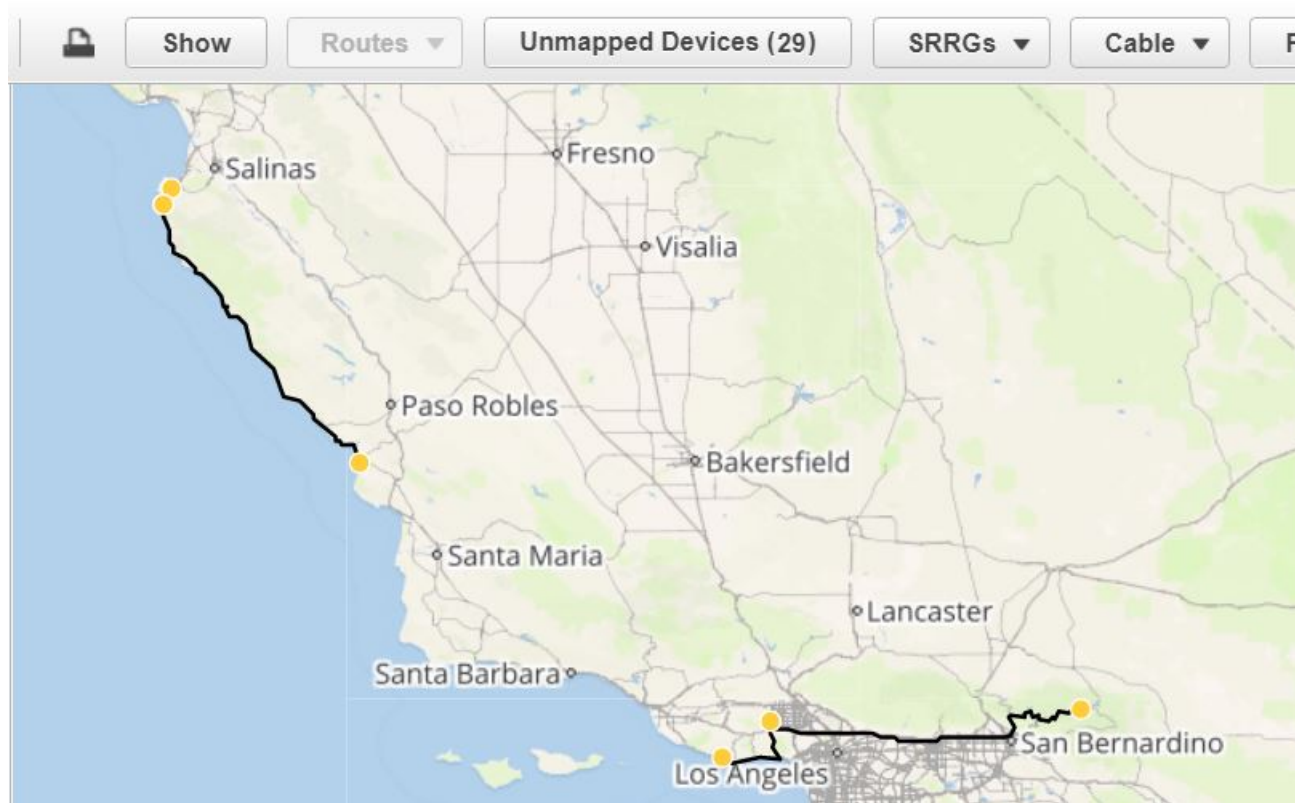
---

## View and Manage Optical Fiber Paths in the Geo Map

To view optical fibers in the geo map, you must create a KML file with the location data for the fibers and import it into Cisco EPN Manager . For information about importing fiber location data, see [Import Location Data from a KML File, on page 185](#).

After you import a KML file that contains fiber location data, the fibers are shown on the geo map. If you do not want to see them on the map, go to **Show > Links** and deselect **Fiber** under Physical Layer links.

Optical fibers are represented as follows in the geo map:



See [Manage Fiber Paths, on page 182](#) and [Associate Links to Fibers, on page 183](#) for information about editing/deleting fibers and associating fibers to links.

## Manage Fiber Paths

Fiber paths that are displayed in the geo map can be edited, deleted, or associated to links in the Fiber Management dialog. Click the **Fibers** button in the geo map toolbar to open the Fiber Management dialog.

Note the following:

- The Fiber Management dialog lists fibers that are currently visible in the map only. If you cannot see the fibers in the geo map, they will not appear in the Fiber Management dialog. Set up your geo map so that the fibers you want to manage are being displayed.
- When you select a fiber in the Fiber Management dialog, the selected fiber is highlighted in purple in the geo map. If the fiber is associated with a link, the link will also be highlighted in purple in the map. When you click on a fiber in the geo map, the fiber is selected in the Fiber Management dialog.
- To show additional details about a specific fiber, click the arrow next to the fiber name to show the fiber description.
- You can edit the fiber name, length (in km), and description. To edit a fiber, select it in the list and click the **Edit** button. Click **Save** when you have completed your edits.
- To delete fibers, select the required fibers and click the **Delete** button.

- If a fiber is associated with a link, a link icon will be present in the Link column. Click on the icon to display the name of the link. You can disassociate the link if necessary. See [Associate Links to Fibers, on page 183](#) for more information.

## Associate Links to Fibers

A fiber can be associated to an OTN or OTS link so that you can visualize both the fiber and its associated link on the map. To associate a fiber to a link, you must populate a KML file with the necessary information and then import the KML file into the system.

A KML template that outlines the format for providing fiber-link associations can be downloaded and then imported after you have added the required information.

To associate a link to a fiber:

- 
- Step 1** Download the KML template that contains the correct KML format and instructions for fiber-link associations:
- Click the **Import** icon in the geo map toolbar and choose **KML**.
  - Download the KML template by clicking the link at the bottom of the displayed dialog.
  - In the KML file, locate the folder called "Links association info". This folder contains the format and instructions for creating a fiber-link association.
- Step 2** Enter the required information in the KML file, save it, and then import it into the system. See [Import Location Data from a KML File, on page 185](#).
- Step 3** In the geo map, check that your fibers are displayed, then click on **Fibers** in the toolbar. In the Fiber Management dialog, the fibers to which you associated links should have a link icon in the Link column. Click on the link icon to see the name of the associated link.
- 

## Visualize Circuits/VCs on the Geo Map

The circuit/VC overlay functionality in the geo map is very similar to overlay in the topology map. However, because of some differences in the functioning of the maps, a few items regarding overlay functionality in the geo map need to be noted:

- To overlay a circuit on the geo map, select the circuit/VC in the Circuits/VCs tab on the left, as you would in the topology map.
- Select the **Show Participating Devices Only** check box to remove all devices from the map except for those participating in the selected circuit/VC.
- Click the **Participating Devices** link to show a list of all the devices participating in the circuit/VC. The list shows the role of the devices, for example, A-side and Z-side, and you can change the location of the devices or remove them from the map.
- If a participating device is in a cluster on the geo map, the badge denoting the role of the device is shown on the cluster icon. Zoom in to see the individual devices so that you can see exactly which device the role badge is marking. Alternatively, click on the **Participating Devices** link to see all the devices and their roles in the circuit/VC.

- If some of the participating devices are not currently displayed on the map, a message will be displayed and will enable you to open the list of unmapped devices. You can place them on the map by dragging and dropping the devices or click **Set Location** and enter their GPS coordinates.

## Import Location Data

In addition to manually placing devices on the geo map, you can specify the coordinates of devices or fibers in an external file and then import the file. The system reads the coordinates from the file and places the devices/fibers on the map. This is useful for locating items on the map in bulk or for transferring location data from another system. You can also export your existing locations from the geo map, make changes, and then import the data back into the system.

You can import:

- Device locations from a CSV or KML file
- Device and fiber path locations and manually-created managed links from a KML file.

Keyhole Markup Language (KML) is a file format used to display geographic data in two- or three-dimensional maps or in Earth browsers like Google Earth. KML is based on the XML standard and uses a tag-based structure with nested elements and attributes.

For both file formats you can download a template from the GUI which will guide you as to the format in which you need to enter the information so that the system can read it. To download the template, click on the Import Locations icon above the geo map, select one of the options, and click on the template link.

See [Import Device Locations from a CSV File, on page 184](#) and [Import Location Data from a KML File, on page 185](#) for more information.

## Import Device Locations from a CSV File

Device locations can be imported from a CSV file. The devices will be placed on the map according to the coordinates you specify in the file.

For CSV file import, GPS coordinates can be specified in any of the following formats:

- Degrees and decimal minutes (DMM): 41 24.2028, 2 10.4418
- Decimal degrees (DD): 41.40338, 2.17403
- Degrees, minutes, and seconds (DMS): 41°24'12.2"N 2°10'26.5"E



### Note

When using DMS format, please use a double quotation mark (") to indicate the seconds.

To import device locations from a CSV file:

- Step 1** Click the **Import Locations** icon in the geo map toolbar and choose **Device locations only (CSV)**.
- Step 2** Optionally download the CSV template by clicking the link at the bottom of the displayed dialog.
- Step 3** Enter the IP address and longitude and latitude coordinates for each device in the CSV file and save it.

Following is an example of the format of the location information in the CSV file:

IP Address	Longitude	Latitude
x.x.x.x	-121.95823	37.41023
x.x.x.x	8 30.175781 e	23* 15' 23.45"" N

**Step 4** In the Import Locations dialog, browse to the location of your .csv file and click **Place Devices**. The devices will be placed on the map in the locations you specified.

## Import Location Data from a KML File

Keyhole Markup Language (KML) is a file format used to display geographic data in two- or three-dimensional maps or in Earth browsers like Google Earth. KML is based on the XML standard and uses a tag-based structure with nested elements and attributes. You can create a KML file with your device and fiber path location data and import it in order to place your devices and fibers on the geo map. The following location data can be included in the KML file:

- Device location data
- Fiber location data
- Fiber to link associations
- Manually-created managed links. After import, the managed links will be displayed in the topology map and in the geo map (if both endpoints of the managed link are "mapped" in the geo map).

A template is provided to guide you as to the required format in which to enter information within the KML file.



**Note** Coordinates must be entered in Decimal degrees (DD) format, for example, 41.40338, 2.17403.

Following is an example of the KML format for device locations:

```
<Placemark>
  <name>454A-234-157</name>
  <Point>
    <coordinates> -121.930938,37.411522</coordinates>
  </Point>
  <ExtendedData>
    <Data name="nodeIpAddress">
      <value>10.56.23.47</value>
    </Data>
  </ExtendedData>
</Placemark>
```

Following is an example of the KML format for fiber paths:

```
<Placemark>
  <name>Fiber-1</name>
  <description>Fiber-1 long description</description>
  <LineString>
    <coordinates> -121.930938,37.411522,0.0 -121.931405,37.413011,0.0 -121.929364,37.413588,0.0
    -121.930973,37.414602,0.0
  </coordinates>
```

```
<LineString>
</Placemark>
```

Following is an example of the KML format for fiber-link associations, where you must:

- Define one link association per folder, with the name "linkAssociation".
- Specify the segments of the fiber in the sequence that follows the A to Z path of the link to be associated.
- Specify the IP address of the A and Z sides of the link to be associated.

```
<Folder>
<name>Links association info</name>
<Folder>
  <name>linksAssociation</name>
  <description>OTS link-1</description>
  <ExtendedData>
    <Data> name="segments">
      <value>Fiber-1,Fiber-1-to-2-segment,Fiber-2</value>
    </Data>
    <Data> name="nodeAIpAddress">
      <value>10.56.23.47</value>
    </Data>
    <Data> name="nodeZIpAddress">
      <value>2001:cdba:0000:0000:0000:0000:3257:9652</value>
    </Data>
    <Data> name="nodeAInterfaceName">
      <value>LINE-2-17-3-TX</value>
    </Data>
    <Data> name="nodeZInterfaceName">
      <value>LINE-1-1-3-TX</value>
    </Data>
    <Data> name="linktype">
      <value>OTS</value>
    </Data>
  </ExtendedData>
</Folder>
</Folder>
```

Following is an example of the KML format for fiber-link associations, where you must:

- Define one link association per folder, with the name "linkAssociation".
- Specify the segments of the fiber in the sequence that follows the A to Z path of the link to be associated.
- Specify the IP address of the A and Z sides of the link to be associated.

```
<Folder>
<name>Links association info</name>
<Folder>
  <name>linksAssociation</name>
  <description>OTS link-1</description>
  <ExtendedData>
    <Data> name="segments">
      <value>Fiber-1,Fiber-1-to-2-segment,Fiber-2</value>
    </Data>
    <Data> name="nodeAIpAddress">
      <value>10.56.23.47</value>
    </Data>
    <Data> name="nodeZIpAddress">
      <value>2001:cdba:0000:0000:0000:0000:3257:9652</value>
```



```

</Data>
<Data> name="nodeAInterfaceName">
  <value>LINE-2-17-3-TX</value>
</Data>
<Data> name="nodeZInterfaceName">
  <value>LINE-1-1-3-TX</value>
</Data>
<Data> name="linktype">
  <value>OTS</value>
</Data>
</ExtendedData>
</Folder>
</Folder>

```

To import location data from a KML file:

- 
- Step 1** Click the **Import** icon in the geo map toolbar and choose **KML**.
  - Step 2** Optionally download the KML template by clicking the link at the bottom of the displayed dialog.
  - Step 3** Create a KML file and enter device/fiber/link data using the format and information in the template as a guide. Save the KML file.
  - Step 4** In the Import KML dialog, browse to the saved KML file and click **Import**. The devices and fibers will be placed on the geo map in the locations you specified. Managed links will be displayed in the topology map. To see the imported managed links in the geo map, make sure that the devices on either side of the link are mapped in the geo map.
- 

## Export Location Data from the Geo Map

You can export location data for devices, fibers, fibers with link associations, and manually-created managed links from the geo map to a KML file. Once you have the data in a KML file, you can edit it as required and then import it back into the geo map.




---

**Note** Fiber location data cannot be exported together with the other location data - it must be exported in a separate operation.

---

- 
- Step 1** Click the **Export KML** icon in the geo map toolbar.
  - Step 2** In the Export Options (KML) dialog, select the location data you want to export. Note that if you select Unassociated Fibers, the other options will be disabled because these fibers must be exported independently of the other location data.
  - Step 3** Click **Export**. A KML file with your selected location data is created.
-

## View and Manage Shared Risk Resource Groups (SRRG) in the Geo Map



**Note** This feature is supported on optical devices and links only, specifically NCS 2000 and NCS 4000 devices and OTS or OTU links.

A Shared Risk Resource Group (SRRG) is a set of devices and links that share a common resource, which if it fails, would affect all the devices and links in the group and the circuits in which they participate. The devices and links in the group share the same risk of failure and are therefore considered to belong to the same SRRG. For example, links sharing a common fiber are said to be in the same SRRG because a fault with the fiber might cause all links in the group to fail.

For devices, the SRRG is configured on the global device level. For links, the same SRRG is configured on the A-side and Z-side interfaces.

In the geo map, you can visualize SRRGs that have been configured on specific devices and discovered by the system. These SRRGs have an auto-generated numeric ID that cannot be changed but you can assign a label to the SRRG to provide a more easily identifiable name. You can also assign SRRGs to specific devices/links, modify SRRG assignments, and create and assign new SRRGs.

SRRG management is accessed from the geo map, from the Shared Risks (SRRGs) button above the map. When managing SRRGs, the map is filtered to show only devices that support SRRG.

See [View Assigned and Unassigned SRRGs, on page 188](#) and [Manage SRRG Assignments, on page 189](#) for more information.

### View Assigned and Unassigned SRRGs

You can view a global list of the SRRGs configured on the managed devices. Since these SRRGs were discovered by the system or user-defined on specific devices or links, they are all "assigned" SRRGs. You can also see unassigned SRRGs. SRRGs can only be deleted from the system if they are unassigned.

Each SRRG has a numeric ID that cannot be changed but you can assign a label to the SRRG to provide a more easily identifiable name.

You can select an SRRG to show the devices/links to which it is assigned in the geo map.

To view and label SRRGs:

- 
- Step 1** In the left sidebar, select **Maps > Topology Maps > Network Topology**.
  - Step 2** Click on the Geographical Map toggle button in the top right corner of the map.
  - Step 3** Click the **Shared Risks (SRRGs)** button above the map and select **View and Name**. The Shared Risk Resource Groups dialog is displayed. It contains two tabs showing assigned and unassigned SRRGs. Note that when viewing SRRG assignments, your device group selection is changed to the default All Locations group.
  - Step 4** Select a SRRG to view it in the geo map. The devices and links on which the SRRG is defined will be highlighted in the map.
  - Step 5** To rename a SRRG, click in the SRRG Label column alongside the relevant SRRG ID, type in the required unique name, and click **Save**.
-

## Manage SRRG Assignments

A simple wizard enables you to select specific devices and links, see which SRRGs are assigned to them and change the assignments as required.

To manage SRRG assignments:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	In the left sidebar, select <b>Maps &gt; Topology Maps &gt; Network Topology</b> .	
<b>Step 2</b>	Click on the Geographical Map toggle button in the top right corner of the map.	
<b>Step 3</b>	Click the <b>Shared Risks (SRRGs)</b> button above the map and select <b>Manage Assignments</b> . The Manage SRRG Assignments wizard opens.	
<b>Step 4</b>	Select the devices/links for which you want to manage SRRG assignments. You can either click on the required devices/links in the map or click in the box in Step 1 of the wizard and select devices from the list.	
<b>Step 5</b>	Click <b>Next</b> . You will see a list of all the SRRGs common to all the devices/links you selected in the previous step. If an SRRG is assigned to one of the selected devices but not to the others, it will not be shown in the list. The SRRGs are color-coded based on whether they are the default on the device, assigned, or yet to be assigned. Click on the question mark icon to see the legend.	
<b>Step 6</b>	Click the Plus icon and select additional SRRGs for the selected devices/links or create a new SRRG on the fly by typing an SRRG name. If the name is unique, a Create New link will appear.	
<b>Step 7</b>	Click <b>Next</b> to see a summary of your selections and SRRG assignments.	
<b>Step 8</b>	Click <b>Finish</b> . You will be notified if the SRRG modification was successful. If it failed, an error dialog will provide details of the failure.	





## PART IV

# Monitor the Network

- [Monitor Device and Network Health and Performance, on page 193](#)
- [Monitor Alarms and Events, on page 213](#)
- [Monitor Cisco ASR 9000 Network Virtualization \(nV\) Satellites and Cluster Services, on page 233](#)
- [Manage Reports, on page 245](#)





## CHAPTER 8

# Monitor Device and Network Health and Performance

---

- [How Device Health and Performance Is Monitored: Monitoring Policies, on page 193](#)
- [Set Up Basic Device Health Monitoring, on page 194](#)
- [Set Up Basic Interface Monitoring, on page 195](#)
- [Use the Dashboards To Check Network and Device Health, on page 197](#)
- [Check What Cisco EPN Manager Is Monitoring, on page 198](#)
- [Check a Monitoring Policy's Device, Polling, Threshold, and Alarm Settings, on page 201](#)
- [Adjust What Is Being Monitored, on page 201](#)
- [Check the Status of Past Monitoring Policy Data Collections, on page 204](#)
- [Change the Device Set a Policy is Monitoring, on page 204](#)
- [Change the Polling for a Monitoring Policy, on page 205](#)
- [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205](#)
- [Run Performance Tests, on page 206](#)
- [Run a Performance Test on a Link \(OTS Link\), on page 207](#)
- [Monitor Network Performance Using Reports, on page 212](#)

## How Device Health and Performance Is Monitored: Monitoring Policies

*Monitoring policies* control how Cisco EPN Manager monitors your network by controlling the following:

- What is monitored—The network and device attributes Cisco EPN Manager monitors.
- How often it is monitored—The rate at which parameters are polled.
- When to indicate a problem—Acceptable values for the polled attributes.
- How to indicate a problem—Whether Cisco EPN Manager should generate an alarm if a threshold is surpassed, and what the alarm severity should be.

Monitoring policies are important because apart from controlling what is monitored, they determine what data can be displayed in reports, dashboards, and other areas of Cisco EPN Manager. Monitoring policies do not make any changes on devices.

Only device health monitoring (that is, the Device Health monitoring policy) is enabled by default. Interface Health monitoring is not enabled by default to protect system performance in large deployments. Note that the Device Health monitoring policy does not apply to the Cisco NCS 2000 and Cisco ONS families of devices. To monitor those device types, use the optical monitoring policies listed in [Monitoring Policies Reference, on page 767](#).

These steps summarize how you can configure a monitoring policy.

1. Use a monitoring **policy type** as a template for your monitoring policy, and give the policy a name that is meaningful to you. Policy types are packaged with Cisco EPN Manager and make it easy for you to start monitoring different technologies and services, such as Quality of Service, Optical SFP, and TDM/SONET. A complete list is provided in [Monitoring Policies Reference, on page 767](#).
2. Adjust your policy's polling frequencies or disable polling altogether for specific parameters.
3. Specify the threshold crossing alarms (TCAs) you want Cisco EPN Manager to generate if a parameter's threshold is surpassed. Some TCAs are configured by default; you can adjust or disable them, and configure new TCAs.
4. Specify the devices you want your policy to monitor. Devices are filtered depending on the policy type.
5. Activate your policy. The polled data will be displayed in dashboards, reports, the Alarms and Events table, and other areas of the web GUI.

To view and administer monitoring policies, choose **Monitor > Monitoring Tools > Monitoring Policies**.

Navigation	Description
<b>Automonitoring</b>	Lists the policies that are enabled by default in Cisco EPN Manager. Only the Device Health monitoring policy is enabled by default. You can adjust the settings for this policy.
<b>My Policies</b>	The policy you create is listed here. When you choose a policy from <b>My Policies</b> , you can view the policy's details.

## Set Up Basic Device Health Monitoring

The Device Health monitoring policy is enabled by default. It checks managed devices for CPU utilization, memory pool utilization, environment temperature, and device availability. This policy also specifies thresholds for utilization and temperature which, if surpassed, trigger alarms that are displayed in the GUI client.

To view the current settings for this policy, choose **Monitor > Monitoring Tools > Monitoring Policies**, then select **Automonitoring** from the list on the left. You can also adjust the polling frequency and threshold for the different parameters. To adjust a polling frequency or threshold, use the drop-down lists that are provided in the GUI client.

You might also want to create a device health monitoring policy that monitors specific devices—for example, devices of a certain type or in a certain geographical location. For instructions on how to do this, see [Adjust What Is Being Monitored, on page 201](#).



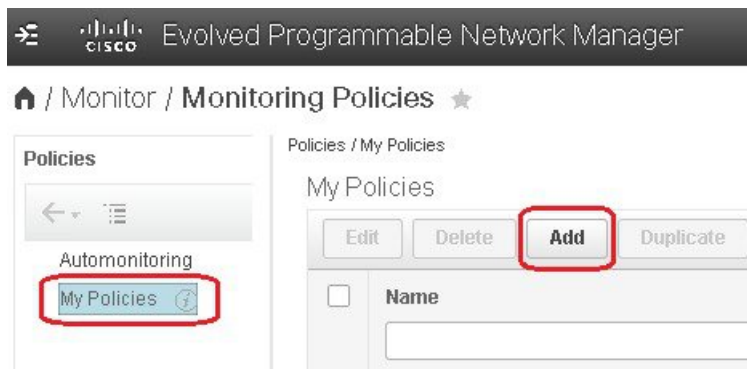
# Set Up Basic Interface Monitoring

Interfaces are not monitored by default. This protects system performance for networks with large numbers of interfaces. Use this procedure to set up basic interface monitoring.

To set up and enable interface monitoring:

**Step 1** Choose **Monitor > Monitoring Tools > Monitoring Policies**, then select **My Policies** from the list on the left.

**Step 2** Click **Add** to create a new policy.



**Step 3** Choose **Interface Health** for generic interface monitoring. If you are monitoring optical devices, choose **Optical 15 Mins** or another optical policy (see [Monitoring Policies Reference, on page 767](#)).

When you select a policy, Cisco EPN Manager populates the window with the policy settings.

**Step 4** Enter a meaningful name and description.

**Step 5** From the **Device Selection** drop-down list, click the appropriate radio button and then select the devices or device groups you want to monitor. If you chose the Interface Health monitoring policy, you can also select port groups.

Cisco EPN Manager only lists the devices or ports applicable to the policy you selected in Step 3.

Note the following:

- If you want to use the default settings for polling and thresholds, proceed to Step 8.
- Due to a limitation in the current release of Cisco EPN Manager, the Interface Health monitoring policy polls all of the interfaces in your network for cyclic redundancy check (CRC) error data, not just the ones associated with the selected port group. Keep this in mind whenever you view CRC error data.

**Step 6** To adjust how often the interface is polled, select a value from the **Polling Frequency** drop-down list. Some policies allow you to set polling frequencies for different parameters, while other policies have only one polling frequency that is applied to all parameters.

For example, the following shows a policy that will monitor Cisco ASR 9000 interfaces. It uses the **Interface Health** policy type, where all parameters are polled using the same interval.

Policies / My Policies

## ASR9K-IF-Health

\*Device Selection ▼

\* Name ASR9K-IF-Health

Author root

Description

Contact

Feature Category Interface Health

Status Active

## Parameters and Thresholds

	Parameter	Polling Frequency	
▶	Statistics	15 min ▼	
▶	CRC	No Polling ▼	

Save and Activate ▼

Cancel

Alternatively, the following shows a policy that will monitor Cisco NCS 2000 interfaces. It uses the **Optical 15 mins** policy type, where each interface type has its own polling interval. You can edit the interval by double-clicking it.

Policy Types / **Optical 15 mins**

\* Device Selection ▼

\* Name NCS-2000-SanJose

Author root

Description Template for collecting  
Optical Statistics (15 mins)

Contact

Feature Category Optical 15 mins

**Parameters and Thresholds**

Parameter	Polling Fre...	
Physical	15 min	
<b>OTN</b>	15 min ▼	
Ethernet	15 min	Save   Cancel
SonetSdh	15 min	
Dwdm Infrastructure	15 min	

Save and Activate ▼

Cancel

**Step 7** If the policy supports TCA customization, you can adjust the thresholds. See [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205](#).

**Step 8** Click:

- **Save and Activate** to start monitoring immediately
- **Save and Close** to save the policy and activate it at a later time

## Use the Dashboards To Check Network and Device Health

Cisco EPN Manager provides a variety of dashboards for monitoring your devices and network. The following are some examples of what dashboards can provide:

- Network-wide real-time status information, such as unreachable devices, interfaces that are down, and the most recent alarms.

- Summarized historical information, such as the most frequently-occurring alarms, and the devices and interfaces with the highest memory and CPU utilization.
- Device-specific information, such as a device's reachability history, utilization, interface statistics, and alarms.
- Technology-specific information, such as Carrier Ethernet services.

For information on dashboards, see [Set Up and Use the Dashboards, on page 6](#).

## Check What Cisco EPN Manager Is Monitoring

This topic explains how to get the following information:

- Which policies are activated, their status, and their history.
- The specific parameters that Cisco EPN Manager is polling, the frequency at which they are polled, and their threshold crossing alarm (TCA) settings.
- Who created the policy and which policy type they used as its basis.

To find out what a policy polls, when the policy last ran, and whether the policy is currently active, choose **Monitor > Monitoring Tools > Monitoring Policies**, then choose **My Policies**. Cisco EPN Manager lists the monitoring policies you created or have access to, with the following information.

Policy Field	Description
Name	Policy name (specified by the policy creator). To find out who created a policy, see the instructions that follow this table.
Description	Policy description (specified by the policy creator).
Type	Template (policy type) used to create this policy. For information on the policy types, see <a href="#">How Device Health and Performance Is Monitored: Monitoring Policies, on page 193</a> .
Status	<b>Active</b> or <b>Inactive</b> .
Threshold	Whether the policy monitors parameter thresholds and generates TCAs. If <b>Yes</b> is displayed, you can check the TCA settings using the instructions that follow this table.

Policy Field	Description
Activation History	<p>Active monitoring policy—Displays the number of times the policy was activated, and provides a hyperlink to an Activation History popup window that tells you:</p> <ul style="list-style-type: none"> <li>• When the policy was activated.</li> <li>• Which devices were polled at each policy run. If the list is very long, hover your mouse cursor over the list in the <b>Activated for</b> column to launch a popup window.</li> </ul> <p>Inactive monitoring policy—Displays <b>Not Available</b>.</p>
Collection Status	<p>Active monitoring policy—Provides a hyperlink to a Collection Status popup window that tells you:</p> <ul style="list-style-type: none"> <li>• The Device name, IP address, and reachability state of each device that was polled by the policy.</li> <li>• Which parameters were polled at each policy run. If the list is very long, hover your mouse cursor over the list in the <b>Parameters</b> column to launch a popup window.</li> </ul> <p>Inactive monitoring policy—Displays <b>Not Available</b>.</p>

To view polling frequencies and TCA details, from **My Policies**, select a policy from the list on the left. Depending on the policy type, the following information is displayed.



**Note** The Optical 1 day and Optical 15 minutes policies do not display polled parameters in the web GUI. That information is provided in [Monitoring Policies Reference, on page 767](#).

Policy Field	Description
General Information	Name, description, creator, status, policy type (Feature Category). For information on the policy types, see <a href="#">How Device Health and Performance Is Monitored: Monitoring Policies, on page 193</a> .
Device Selection	Devices which the policy is monitoring.
Polling Frequency	How often Cisco EPN Manager polls the device parameters.

Policy Field	Description
Parameters and Thresholds	Which parameters are polled and their TCA settings, if any. To view the TCA settings, click the arrow next to the parameter name. For more information about viewing the parameters polled by the various policy types, see <a href="#">Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 200</a> .

## Check Which Parameters and Counters Are Polled By a Monitoring Policy

[Check What Cisco EPN Manager Is Monitoring, on page 198](#) explains how to find out which monitoring policies are currently activated. To find out which *parameters* are being polled by a policy, follow this procedure.



### Note

Because Optical 1 Day and Optical 15 Mins parameters are not displayed in the web GUI, they are listed in [Monitoring Policies Reference, on page 767](#).

You can use this procedure to check:

- Parameters polled by existing policies (regardless of whether a policy is active or inactive).
- Parameters used by a policy type. This useful if you want to check what a new policy will poll before creating the policy.

**Step 1** Choose **Monitor > Monitoring Tools > Monitoring Policies**, then choose **My Policies**. The web GUI lists the existing active and inactive monitoring policies.

**Step 2** **To check the parameters used by an existing policy:**

- To view parameters that were polled most recently, locate the policy in the window on the right, then click **Details** in the **Collection Status** column. In the Collection Data dialog box, hover your mouse over the text in the **Parameter** column to list the polled parameters.
- To view the parameters along with their polling settings, expand **My Policies** in the navigation area on the left, then choose the policy you want to check. The window on the right displays the parameters and their polling settings.

**Step 3** **To check the parameters used by a specific policy type:**

- Click **Edit**. The supported policy types are listed in the navigation area on the left.
- Choose a policy type. The window on the right displays the parameters polled by that policy, along with default polling and TCA settings. (These settings can be customized when a monitoring policy is created.)

## Policies Pane Pop-Up Window

From the **Policies** pane in the **Monitoring Policies** page, you can open a pop-up window that provides summary information and action links for the corresponding policy or policy folder. To open a pop-up window, place your cursor over the appropriate *i* (**information**) icon.

- If you open the pop-up window for a policy, it displays information such as the policy's type, status, and timestamp for the last time it was updated. From the **Actions** area, you can click links to edit, delete, or duplicate the policy.
- If you open the pop-up window for a policy folder, it indicates the folder's name and the number of policies that belong to it. From the **Actions** area, you can click links to delete the folder or add a new sub-folder. Note that you can only add and delete folders within **My Policies**. Also, when user-created folders are in place, you need to specify the destination folder whenever you create a new policy.

## Check a Monitoring Policy's Device, Polling, Threshold, and Alarm Settings

To check a monitoring policy's threshold and alarm settings:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Monitor</b> > <b>Monitoring Tools</b> > <b>Monitoring Policies</b> , then choose <b>My Policies</b> .                                                                                                                                                                                                                                                                                 |
| <b>Step 2</b> | Select the monitoring policy and click <b>Edit</b> to open the policy details.                                                                                                                                                                                                                                                                                                                  |
| <b>Step 3</b> | To find out which devices the policy is monitoring, click the <b>Device Selection</b> drop-down list. Devices that are monitored are indicated with a check mark. To add or remove devices, see <a href="#">Change the Device Set a Policy is Monitoring, on page 204</a> .                                                                                                                     |
| <b>Step 4</b> | To find out the polling interval the policy is using, check the <b>Polling Interval</b> setting. For per-parameter polling, you must expand the individual parameters to see the setting. To adjust the polling settings, see <a href="#">Change the Polling for a Monitoring Policy, on page 205</a> .<br><br>Optical policy polling frequencies cannot be changed; they can only be disabled. |
| <b>Step 5</b> | To find out the thresholds and alarm settings the policy is using, expand the parameter in the <b>Polling and Thresholds</b> area. To change the threshold and alarm settings, see <a href="#">Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205</a> .<br><br>Optical policy thresholds cannot be customized.                                                           |
- 

## Adjust What Is Being Monitored

To make adjustments to what Cisco EPN Manager is monitoring, use the guidance in the following table to find the best method for your needs.

If:		See:
Cisco EPN Manager is collecting the data you need, and...	... you want to change the polling frequency	<a href="#">Change the Polling for a Monitoring Policy, on page 205</a>
	... you want to adjust the alarm behavior	<a href="#">Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205</a>
	... you want to adjust which devices are monitored	<a href="#">Change the Device Set a Policy is Monitoring, on page 204</a>
Cisco EPN Manager is <i>not</i> collecting the data you need, and...	... a similar monitoring policy already exists	<a href="#">Create a New Monitoring Policy Based On An Existing Policy, on page 202</a>
	... no similar monitoring policies exist, but one of the policy types contains the parameters you want to monitor	<a href="#">Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203</a>
	... no similar monitoring policies exist, and none of the policy types contain the parameters you want to monitor	<a href="#">Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 203</a>
	... you want it to monitor unsupported or third-party devices	

## Create a New Monitoring Policy Based On An Existing Policy

- Step 1** Check what is currently being monitored to verify that you need to create a new policy. See [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- Step 2** Create the duplicate.
- Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then click **My Policies** from the list on the left.
  - Locate the policy you want to duplicate.
  - Select the policy, then click **Duplicate**.
  - In the **Duplicate Policy Creation** dialog, choose the parent folder, enter a policy name and description, then click **OK**.
- Step 3** Make your changes to the duplicate.
- Locate the policy under **My Policies**.
  - Select the policy and click **Edit**.
  - Make your changes as needed. See:
    - [Change the Device Set a Policy is Monitoring, on page 204](#)
    - [Change the Polling for a Monitoring Policy, on page 205](#)
    - [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205](#)
- Step 4** Click:
- **Save and Activate** to save and activate the policy immediately on the selected devices.



- **Save and Close** to save the policy and activate it at a later time.

---

## Create a New Monitoring Policy Using Out-of-the-Box Policy Types

---

- Step 1** Check what is currently being monitored. See [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- Step 2** Choose **Monitor > Monitoring Tools > Monitoring Policies**, then click **Add**.
- Step 3** Select the policy type template you want to use from the **Policy Types** menu.
- Step 4** Configure the new policy:
- a) Select the devices, device groups, or port groups from the **Device Selection** drop-down list. (Not all monitoring types can be applied to port groups.)
  - b) Enter a name and contact, and edit the description.
  - c) Under **Parameters and Thresholds**, configure the polling settings, parameter values, and alarm conditions. See [Change the Polling for a Monitoring Policy, on page 205](#) and [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205](#).
- Step 5** Click:
- **Save and Activate** to save and activate the policy immediately on the selected devices.
  - **Save and Close** to save the policy and activate it at a later time.
- 

## Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices

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

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

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

You can create a maximum of 25 custom MIB polling policies.

To create a custom MIB polling policies, follow these steps:

- 
- Step 1** Choose **Monitor > Monitoring Tools > Monitoring Policies**, then choose **My Policies** and click **Add**.
- Step 2** From the **Policy Types** menu, select **Custom MIB Polling**.
- Step 3** Enter a name for the policy.

- Step 4** Under the **MIB Selection** tab, specify the polling frequency and enter the MIB information.
- If Cisco EPN Manager does not list the MIB you want to monitor in the MIBs drop-down list, download the MIBs you want to monitor from the following URL:  
<http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2>
  - To upload a MIB, specify a filename extension only if you are uploading a ZIP file.
  - If you are uploading a ZIP file, ensure that all dependent MIB files are either included in the ZIP or already present in the system.
  - Ensure your upload file and the MIB definition have the same name. If you are uploading a ZIP file, you may name it as you please, but the MIB files packaged inside it must also follow the same convention (for example: MyMibs.zip is acceptable, as long as all MIB files in the ZIP match their MIB names).
- Step 5** To test the policy you created on a device before activating it, click the **Test** tab and select a device on which to test the new policy.
- Step 6** Click **Save and Activate** to immediately activate the policy on the devices specified.
- Step 7** To view the MIB polling data, create a generic dashlet on the Performance dashboard using the name of the policy that you created.
- Note** To view the SNMP polling data for Cisco ASR devices, you should use the show platform hardware qfp active datapath utilization | inc Processing command for CPU utilization and show platform hardware qfp active infrastructure exmem statistics | sec DRAM command for memory utilization.

## Check the Status of Past Monitoring Policy Data Collections

To check a monitoring policy's past data collection:

- Step 1** Choose **Monitor > Monitoring Tools > Monitoring Policies**, then click **My Policies**.
- Step 2** Locate the policy, and under the **Collection Status**, click **Details** to open the Collection Data dialog. To see which parameters were polled for a device, hover your mouse over the text in the Parameter column.

## Change the Device Set a Policy is Monitoring

You can customize how often monitoring information is gathered (polling interval). Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

- Step 1** Choose **Monitor > Monitoring Policies > My Policies** and select the policy you want to edit.
- Step 2** Check the policy you want to edit and click **Edit**.
- Step 3** Click the Device Selection drop-down list.
- Step 4** Select and deselect devices as needed.

**Step 5** Click **Save and Activate** to save and activate the policy immediately on the selected devices.

---

## Change the Polling for a Monitoring Policy

You can customize how often monitoring information is gathered (polling interval). Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

---

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

**Step 2** Select the policy you want to edit and click **Edit**.

**Step 3** Adjust the polling frequency. How to adjust polling depends on the monitoring policy type.

- Policies with one polling frequency that applies to all attributes—To adjust the polling frequency, select the new interval from the Polling Frequency drop-down list. To disable polling, deactivate the policy by clicking **Save and Deactivate** at the bottom of the page.
- Policies with per-attribute polling frequencies—To change the polling setting for a specific attribute, double-click the attribute line and change the setting. Choosing **No Polling** will disable polling for that attribute only.

To disable polling for all attributes in the policy, deactivate the policy by clicking **Save and Deactivate** at the bottom of the page. Do not proceed to the next step.

**Step 4** Click **Save and Activate** to save and activate the policy immediately on the selected devices.

---

## Change Thresholds and Alarm Behavior for a Monitoring Policy

You can customize the threshold value that indicates a problem and whether Cisco EPN Manager should generate an informational event or an alarm (of any severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

---

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

**Step 2** Select the policy you want to edit and click **Edit**.

**Step 3** Locate the parameter you want to change. You can search for the parameter by entering a string in the **Parameter** text box.

**Step 4** Expand the parameter. You can change an existing condition or add new conditions, as in the following figure, which specifies thresholds and alarms for CPU utilization on Cisco ASR 9000 devices.

**Step 5** When you are done, click **Save and Activate** to save and activate the policy immediately on the selected devices.

When you run a performance test, Cisco EPN Manager connects to the network devices in real time to retrieve the information. Reports, on the other hand, use historical data that is saved in the database. See these topics for more information, depending upon the type of test you want to run:

- Cisco EPN Manager also supports running OTDR performance tests on OTS optical links. For more information, see [Run a Performance Test on a Link \(OTS Link\), on page 207](#).

## Run a Performance Test on a Link (OTS Link)

An Optical Time Domain Reflectometer (OTDR) test enables you to remotely diagnose OTS link related issues (such as degraded devices, splices and bends in the cables) and supports troubleshooting. OTDR test can be initiated only on the OTS links that are connected to the OTDR port in the TNC card.

The following table lists the different user groups and their privileges:

User Group		Can view OTDR scan? <sup>1</sup>	Can run and analyze OTDR scan? <sup>2</sup>	Can configure OTDR scan? <sup>3</sup>
Web GUI	Root	Yes	Yes	Yes
	Super Users	Yes	Yes	Yes
	Admin	Yes	Yes	Yes
	Config Managers	Yes	Yes	Yes
	System Monitoring	Yes	Yes	No

1. Users who can only view the scan results are not allowed to run the scan or perform any configuration changes.

2. Users who can run and analyze the scan results are not allowed to set baseline or perform any configuration changes.

3. User who can configure the scan are allowed to perform all the actions such as viewing the scan results, setting baseline and so on.

The following procedures describe how to configure and run the OTDR test in the OTDR ports of the TNC cards:

- 
- Step 1**     [Configure OTDR Port Values, on page 207](#)
  - Step 2**     [Provision OTDR Scan Recurrence, on page 209](#)
  - Step 3**     [Run the OTDR Test, on page 209](#)
  - Step 4**     [Export the OTDR Scan Result, on page 210](#)
- 

## Configure OTDR Port Values

This task configures the OTDR equipment values on TNCS cards for each sector required for the OTDR scan.

- 
- Step 1**     From the left sidebar, choose **Inventory > Other > Links**.
  - Step 2**     Select the OTS link, click **Actions**, and then click **OTDR scan**.

You can also launch **OTDR scan** from the following 360 views:

- Topology Maps - Link 360 View:
  1. From the left sidebar, choose **Maps > Topology Maps > Network Topology** and click the **Links** tab. The Links table with all the links will be displayed.
  2. In the Links table, and click the "i" icon next to the OTS link name. Link 360 view is launched.

3. In the Link 360 view, choose **Actions** > **OTDR scan**.

• Interface 360 View:

1. Click the **Interface** tab in the Device 360 or Circuit/VC 360 view.
2. Click the "i" icon next to the interface name. Interface 360 view is launched.
3. In the Interface 360 view, choose **Actions** > **OTDR scan**.

**Step 3** In the **Configure** tab, select a device from the **Device** drop-down list. A table is displayed listing all the sectors with the default values for the following columns:

- Scan Status—Cumulative status of the scans
- Loss Sensitivity (dB)
- Reflection Sensitivity (dB)
- Start Point (km)
- End Point (km)
- Pulse Width (microseconds)
- Resolution (m)
- Measure Time (s)
- Baseline—Baseline is not set by default
- Threshold Loss (dB)
- Threshold Reflection (dB)
- Recurrence—Recurrence is not set by default

The OTDR measurement ranges are categorized based on the fiber spans defined for each sector. Following are the OTDR measurement sectors:

- **Zone #1**—Distance 0 to 1 km
- **Zone #2**—Distance 0 to 25 km
- **Zone #3**—Distance 0 to 80 km
- **Zone #4**—Full distance
- **Expert Mode**—For custom distance settings, you can edit the start point and end point parameters
- **Auto Mode (System Detect)**—The end point parameter is defined automatically

**Note** The distance profiles parameters listed in the **Configure** tab are refreshed for every 30 seconds.

**Step 4** To modify the OTDR settings, click the **Device OTDR Settings** hyperlink. For more details on the OTDR settings, see the 'Configuring OTDR Auto Scan' section in [Provision Optical Interfaces](#), on page 305.

**Step 5** To edit the sector parameters, select the required Distance Profile in the table, and click **Edit**. A popup window is displayed.

**Step 6** In the popup window:

- For **Zone #1** to **Zone #4**—You can edit Loss Sensitivity (dB) and Reflection Sensitivity (dB), Threshold Loss (dB), Threshold Reflection (dB), and Recurrence values. For information on setting the scan recurrence, see [Provision OTDR Scan Recurrence, on page 209](#).
- For **Expert Mode**—You can edit all the columns in the table, except scan status and baseline.
- For **Auto Mode**—You can edit Loss Sensitivity (dB) and Reflection Sensitivity (dB), Threshold Loss (dB), Threshold Reflection (dB), and Recurrence values. The End Point value (length of the fiber span for OTDR scan) is defined automatically. The other values for the scan (Pulse Width, Measure Time, and Resolution) are then configured based on the detected length of the fiber span.

To enable absolute threshold, you need to select Absolute Fiber Pass Fail Criteria check-box in the **OTDR Settings** page.

**Step 7** Click **Save**.

---

## Provision OTDR Scan Recurrence

Follow the below procedure to set up OTDR scan recurrence on the selected ports:

- 
- Step 1** In the **Configure** tab of the OTDR Scans page, from the **Device** drop-down list, select the port on which you want to provision a recurring scan.
- Step 2** Select the appropriate distance profile, and click **Edit**. A popup window is displayed.
- Step 3** In the **Recurrence** area, set the scan frequency by choosing one of the following:
- **None**—No recurrence is set (default).
  - **Weekly**—To schedule a weekly recurring scan, go to [Step 4, on page 209](#).
  - **Intervals**—To schedule a granular recurring scan, go to [Step 5, on page 209](#).
- Step 4** Select the desired day from the **on** drop-down list and enter the hours and minutes.
- Step 5** Select the desired day range between 0 to 365 and enter the hours and minutes.
- Step 6** Click **Save**.
- 

## Run the OTDR Test

Follow the below procedure to run the OTDR test on an OTS Link:

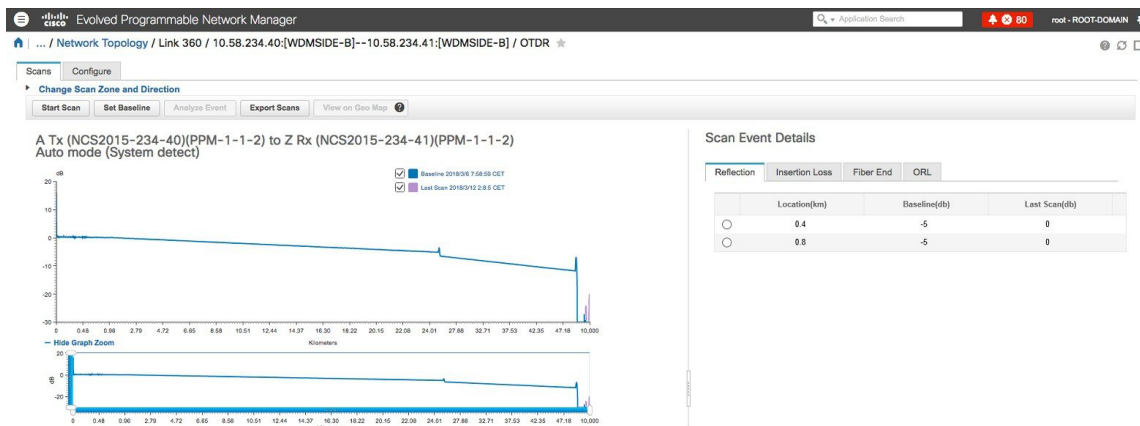
- 
- Step 1** Select the required sector from the **Distance Profile** drop-down list.
- Step 2** In the **Scans** tab, under Scan Direction, select the direction of the test by clicking on the relevant arrow. Note that above each direction arrow is information indicating when the last scan for that direction was run.
- Step 3** Click **Start Scan**.
- A graphical representation of the scan result is displayed with the power readings (dB) over a specified distance profile (km). You can also view the baseline graph to compare with the last scan reading.

## Export the OTDR Scan Result

- A tabular representation of the reflection, loss, fiber end and ORL events for the selected direction and distance profile (sector) is displayed in the **Scan event details** area. Note that fiber end and ORL information is only available for devices running ONS 10.8.
- The Reflection and Loss events tabs display a table with the distance (km), baseline reading (dB) and previous scan reading (dB). They display the relative/absolute threshold, which is the comparison of the baseline to the scan results. You can analyze an event by selecting the event in the table and clicking **Analyze Event**. This causes the scan to be re-run with the specific location of the event.

**Note** An alarm is raised if the threshold exceeds the value set on the device.

- Click **View on Geo Map** to see the scan results within the context of the geo map. See [View OTDR Scan Results in the Geo Map, on page 211](#)



**Step 4** (Optional) Click **Set Baseline** to set an OTDR test baseline. Setting a baseline helps you to compare with the last scan results.

**Step 5** To export the scan results, see [Export the OTDR Scan Result, on page 210](#).

## Export the OTDR Scan Result

You can export the scan results to your local.

**Step 1** Click **Export Scans**.

**Step 2** The currently selected directions and the distance profile will be auto-populated. You can also select the directions and the distance profile for which you need to export the scan result.



- Step 3** Click **Export**. The exported file will be downloaded and saved to your local machine.
- The current version of Cisco EPN Manager supports only the .sor format.

## View OTDR Scan Results in the Geo Map

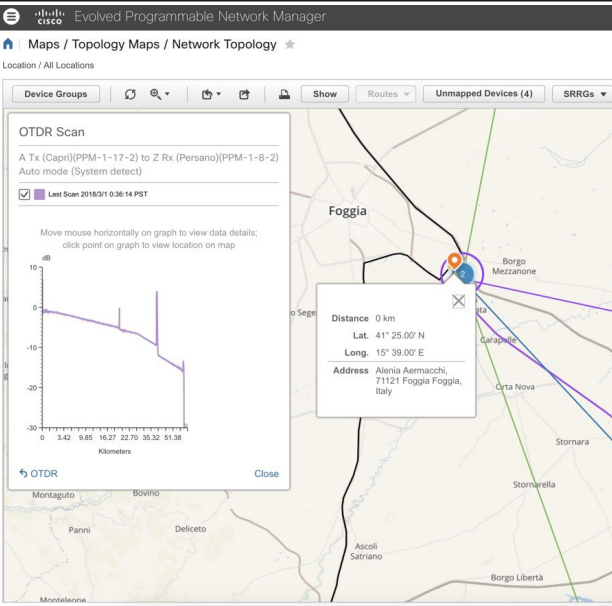
You can view the OTDR scan results in the context of the geo map in order to pinpoint the location of the fiber issues. For example, if the OTDR test reports a concentrated loss 20 km from the link endpoint, you can visualize on the map where this is geographically located.

Prerequisites:

- KML file containing fiber data and coordinates must be imported so that the fibers are visible on the geo map. See [Import Location Data from a KML File, on page 185](#).
- The OTS link on which the OTDR scan is run must be associated with a fiber. See [Associate Links to Fibers, on page 183](#).
- The A- and Z-side devices must be mapped on the geo map. See [Place Unmapped Devices on the Geo Map, on page 178](#).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Launch the OTDR scan.	
<b>Step 2</b>	Define the scan parameters and run the scan.	
<b>Step 3</b>	Click <b>View on Geo Map</b> .	The geo map opens. The OTDR scan results graph is displayed on the left. The geo map zooms to show the relevant devices, link and fiber (highlighted in purple).
<b>Step 4</b>	Click on a point in the OTDR scan results graph.	<p>A location icon appears on the exact location on the fiber on the geo map and a popup panel provides information about that location, including the distance in kilometers along the fiber, the exact coordinates, and the physical address.</p> <p><b>Note</b> If the exact location cannot be calculated, the location icon shows an approximate location that is within a certain radius of the exact location. The radius (in km) is shown in the popup panel and a circle around the location icon in the map indicates that this is an approximate location within a radius of the exact location.</p>

	Command or Action	Purpose
		
<b>Step 5</b>	If necessary, click on the <b>OTDR</b> link below the OTDR scan results graph to return to the OTDR scan page.	

## Monitor Network Performance Using Reports

Cisco EPN Manager provides a variety of reports to help you monitor your network's performance. The following are some examples:

- Environmental temperature, CPU and memory utilization
- Interface errors and discards
- For Carrier Ethernet devices—IPSLA Ethernet OAM, PWE3, QoS, and other CE reports
- For Optical devices—Ethernet, OTN, SDH/SONET, and other optical reports

When you run a performance report, retrieves historical data that has been saved in the database. Reports can only display data that Cisco EPN Manager has been configured to collect—in other words, data that is collected and monitored using monitoring policies. (No monitoring policies have to be enabled for event and alarm-related reports; that data is collected automatically.) For information on which monitoring policies must be enabled for the different reports, see [Available Reports](#), on page 245.



## CHAPTER 9

# Monitor Alarms and Events

- [What Are Alarms and Events?](#), on page 213
- [How are Alarms and Events Created and Updated?](#), on page 214
- [Which Events Are Supported?](#), on page 217
- [Set Alarm and Event Management Preferences](#), on page 217
- [Interpret Event and Alarm Badges and Colors](#), on page 221
- [Find and View Alarms](#), on page 221
- [View a Specific Alarm in the Topology Map](#), on page 223
- [View Root Cause and Correlated Alarms](#), on page 224
- [Get Troubleshooting and Detailed Alarm Information](#), on page 225
- [Acknowledge and Clear Alarms](#), on page 227
- [Add Notes To an Alarm](#), on page 228
- [Forward Alarms and Events as Email Notifications](#), on page 229
- [Manage How Alarms are Triggered \(Alarm Thresholds\)](#), on page 229
- [View Events \(Including Generic Events\)](#), on page 230
- [View Syslogs \(Historic\)](#), on page 230
- [Export Alarms or Events to a CSV or PDF File](#), on page 232
- [Get Support from Cisco](#), on page 232
- [Respond to Problems Within Cisco EPN Manager](#) , on page 232

## What Are Alarms and Events?

An *event* is a distinct incident that occurs at a specific point in time, such as a port status change, or a device becoming unreachable. Events can indicate an errors, failures, or exceptional conditions in the network. Events can also indicate the *clearing* of those errors, failures, or conditions. Event have associated severities (which you can adjust as described in [Change Event Severity Levels](#), on page 709).

An *alarm* is a Cisco EPN Manager response to one or more related events. Only certain events generate alarms. Alarms have a state (cleared or not cleared) and a severity (Critical, Major, Minor, and so forth). An alarm inherits the severity of its most recent event. Alarms remain open until a clearing event is generated (or if the alarm is manually cleared).

### Related Topics

- [How are Alarms and Events Created and Updated?](#), on page 214
- [Acknowledge and Clear Alarms](#), on page 227
- [Interpret Event and Alarm Badges and Colors](#), on page 221

The Cisco EPN Manager processes SNMP traps, syslogs, and TL1 messages from both IPv4 and IPv6 devices. It maintains an event catalog that determines how it should respond to these events. The flowchart below represents the manner in which these alarms and events are processed:

```

graph TD
    Start([Incoming trap or syslog]) --> D1{Is device sending the trap/syslog managed in EPNM}
    D1 -- No --> Drop([Drop the trap/syslog. Do not process any further])
    D1 -- Yes --> D2{Is higher level processing supported for this trap/syslog}
    D2 -- No --> Basic[Do basic processing: convert trap or syslog to 'epnm' 'generic event' with severity = 'MINOR' 'generic event' is shown in 'Event tab']
    D2 -- Yes --> Convert[Convert trap or syslog to 'epnm event'. 'epnm event' is shown in the 'Event tab']
    Convert --> D3{Is above event's severity configured in EPNM 'Alarm Severity' configuration page as INFO}
    D3 -- No --> D4{Does an active alarm (uncleared alarm) exist for this event in EPNM?}
    D4 -- No --> Create[Create an alarm and associate event to Alarm. Set event's severity and description as alarm's severity and description (Note: an alarm is a container for events) 'alarm' is shown in the 'Alarm' tab]
    Create --> D5{Does the alarm participate in PCA/Alarm correlation?}
    D5 -- Yes --> Correl[Perform alarm correlation and update alarm with correlation results. Correlation results are seen in the 'alarm tab's 'correlation type' column and 'correlated alarms tab']
    Correl --> D6{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D6 -- Yes --> Send1[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D6 -- No --> D7{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D7 -- Yes --> Send2[Send alarm update with correlation details northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D7 -- No --> D8{Is alarm's 'category' = 'GENERIC' configured/enabled in 'Notification Receiver' page?}
    D8 -- Yes --> Send3[Send 'generic event northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D8 -- No --> Drop
    D3 -- Yes --> D9{Is Severity = INFO and event's 'category' configured/enabled in 'Notification Receiver' page?}
    D9 -- Yes --> Send4[Send event northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D9 -- No --> D10{Is the alarm flapping or duplicating?}
    D10 -- Yes --> Update1[Update alarm description to indicate flapping/duplicating. Drop further events for this alarm and suppress further updates to this alarm until flapping or duplicating condition stops 'alarm' is shown in the 'Alarm' tab]
    Update1 --> D11{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D11 -- Yes --> Send5[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D11 -- No --> D12{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D12 -- Yes --> Send6[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D12 -- No --> Update2[Update existing alarm with the event's severity and description (Note: an alarm is a container for events) 'alarm' is shown in the 'Alarm' tab]
    Update2 --> D13{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D13 -- Yes --> Send7[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D13 -- No --> D14{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D14 -- Yes --> Send8[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D14 -- No --> D15{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D15 -- Yes --> Send9[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D15 -- No --> D16{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D16 -- Yes --> Send10[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D16 -- No --> D17{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D17 -- Yes --> Send11[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D17 -- No --> D18{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D18 -- Yes --> Send12[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D18 -- No --> D19{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D19 -- Yes --> Send13[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D19 -- No --> D20{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D20 -- Yes --> Send14[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D20 -- No --> D21{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D21 -- Yes --> Send15[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D21 -- No --> D22{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D22 -- Yes --> Send16[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D22 -- No --> D23{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D23 -- Yes --> Send17[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D23 -- No --> D24{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D24 -- Yes --> Send18[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D24 -- No --> D25{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D25 -- Yes --> Send19[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D25 -- No --> D26{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D26 -- Yes --> Send20[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D26 -- No --> D27{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D27 -- Yes --> Send21[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D27 -- No --> D28{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D28 -- Yes --> Send22[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D28 -- No --> D29{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D29 -- Yes --> Send23[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D29 -- No --> D30{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D30 -- Yes --> Send24[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D30 -- No --> D31{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D31 -- Yes --> Send25[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D31 -- No --> D32{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D32 -- Yes --> Send26[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D32 -- No --> D33{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D33 -- Yes --> Send27[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D33 -- No --> D34{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D34 -- Yes --> Send28[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D34 -- No --> D35{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D35 -- Yes --> Send29[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D35 -- No --> D36{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D36 -- Yes --> Send30[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D36 -- No --> D37{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D37 -- Yes --> Send31[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D37 -- No --> D38{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D38 -- Yes --> Send32[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D38 -- No --> D39{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D39 -- Yes --> Send33[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D39 -- No --> D40{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D40 -- Yes --> Send34[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D40 -- No --> D41{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D41 -- Yes --> Send35[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D41 -- No --> D42{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D42 -- Yes --> Send36[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D42 -- No --> D43{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D43 -- Yes --> Send37[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D43 -- No --> D44{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D44 -- Yes --> Send38[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D44 -- No --> D45{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D45 -- Yes --> Send39[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D45 -- No --> D46{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D46 -- Yes --> Send40[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D46 -- No --> D47{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D47 -- Yes --> Send41[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D47 -- No --> D48{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D48 -- Yes --> Send42[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D48 -- No --> D49{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D49 -- Yes --> Send43[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D49 -- No --> D50{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D50 -- Yes --> Send44[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D50 -- No --> D51{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D51 -- Yes --> Send45[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D51 -- No --> D52{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D52 -- Yes --> Send46[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D52 -- No --> D53{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D53 -- Yes --> Send47[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D53 -- No --> D54{Is alarm's 'category' AND severity configured/enabled in 'Notification Receiver' page?}
    D54 -- Yes --> Send48[Send alarm northbound as a trap using CISCO-EPM-NOTIFICATION-MIB]
    D54 -- No --> D55{Is alarm's 'category' AND severity configured/enabled in 'Notification
```

1. Checks the event catalog to see if higher level processing is necessary (as opposed to just generic processing) for the incoming SNMP trap, syslog, or TL1 message (by examining the raw event for predefined patterns).

- If it cannot match the raw event to the catalog, the event is considered a *generic* event and it undergoes generic processing. Generic events are displayed events in the GUI and can be forwarded in notifications. (Generic event handling can be disabled; see [Disable and Enable Generic Trap and Syslog Handling, on page 712](#)). This is done so that none of the traps and syslogs received by Cisco EPN Manager is discarded i.e., they either go through generic processing to create generic events or higher level processing to create alarms/processed events.
- If it can match the raw event to the catalog, the raw event is considered for higher level processing and Cisco EPN Manager creates a processed event with a severity and potentially an alarm.

- 214

3. Checks whether the supported event triggers inventory collection.

Some events have specific rules that instruct Cisco EPN Manager what information it should collect. For more information, see [How Is Inventory Collected?, on page 33](#)

4. Checks whether the event severity is INFO or CLEARED.

- If it is INFO or CLEARED, Cisco EPN Manager saves the event and displays it in the GUI.
- If it is any other severity, Cisco EPN Manager evaluates whether a new alarm should be opened (next step).

5. Checks whether an alarm already exists or a new alarm should be created.

- If an alarm does exist, Cisco EPN Manager associates the event to the existing alarm. The alarm severity is changed to match the severity of the new event, and the alarm time stamp is updated. If it is a clearing event (for example, a link up event), the alarm will be cleared.



---

**Note** In some cases, a device may not generate a clearing alarm. The administrator should set the alarm auto-clearing interval as described in [Change Alarm Auto-Clear Intervals, on page 710](#).

---

- If an alarm does not exist, Cisco EPN Manager creates a new alarm and assigns it the same severity as the event.

6. Checks whether the new or existing alarm can be correlated to any other alarms. (Note that here, alarms are being correlated with other alarms, not with events.) If they can be correlated, Cisco EPN Manager does the following:

- Identifies the causing alarm as the **root cause alarm**.
- Identifies the resulting alarm as a **symptom alarm**.

You can identify uncleared correlated alarms by checking the Correlated Alarms tab in the Alarms and Events table. For more information on these kinds of alarms, see [View Root Cause and Correlated Alarms, on page 224](#).

## Example: Link Down Alarm

In this example, Cisco EPN Manager receives a Link Down trap that it receives from a device. Cisco EPN Manager generates a Link Down event and, because the port is operationally down, it also generates a Link Down alarm. (Cisco EPN Manager will not open an alarm when a port is simply issued a shutdown command.)

Device Groups  
All Devices

Alarms Events Syslogs Cleared Alarms

Showing Latest 4000 Alarms [Show All](#) Selected 0 / To

Change Status Change State Assign Annotation Show Quick Filter

	Severity	Message	Status	Failure Source	Times
<input type="checkbox"/>	Critical	Port 'GigabitEthernet0/3/0/2'...	Not Ack...	prime-asr9010-3.cisco.com	Septen

**General Information**

Source 172.23.222.254

Acknowledged No

Category Routers

Alarm Found At September 14, 2015 7:52:14 PM PDT

Alarm Last Updated At September 14, 2015 9:26:12 PM PDT

Alarm Detected Through Wired Switch

Severity Critical

When Cisco EPN Manager receives a Link Up trap from the device, it generates a Link Up event and clears the alarm.

Device Groups  
All Devices

Alarms Events Syslogs Cleared Alarms

Showing Latest 4000 Cleared Alarms [Show All](#) Selected 0 / Total

Annotation Delete Show Quick Filter

	Severity	Message	Status	Failure Source
<input type="checkbox"/>	Cleared	Port 'GigabitEthernet0/3/0/2' is up on device '172.23.222.254'.	Not Ack...	prime-asr9010-3...

**General Information**

Source 172.23.222.254

Acknowledged No

Category Routers

Alarm Found At September 14, 2015 7:52:14 PM PDT

Alarm Last Updated At September 15, 2015 3:32:48 PM PDT

Alarm Detected Through Wired Switch

Severity Cleared

## Flapping Events and Flow Controllers

Flapping is a flood of consecutive event notifications related to the same alarm. It can occur when a fault causes repeated event notifications (for example, a cable with a loosely fitting connector.) An event is identified as a flapping event if multiple events are of the same type, are associated with the same source, and recur in a short period of time. Cisco EPN Manager will generate an alarm for flapping events. This alarm is generated when there are five occurrences of the same event within 300 seconds. The five occurrences could be of a sequence such as, Interface Down, Interface Up, Interface Down, Interface Up, Interface Down, and so on.

When an alarm is generated for a flapping event, the devices often go into a continuous synchronization state. This can prevent deployment of device configuration such as service provisioning, OAM, etc, on the device. However, in Cisco EPN Manager, when a monitored device raises a Flapping alarm, Cisco EPN Manager detects this alarm and stops further updates of the alarm until the flapping condition on the device is cleared.

The alarm detected as a Flapping Event is cleared based on an exit condition, which is that when there is no occurrence of the same event within the next 300 seconds, the alarm is cleared. This helps control the flow of events to avoid unnecessary triggering of device synchronization.

Device Groups  
All Devices

Alarms Events Syslogs Cleared Alarms

Showing All Events [Show Latest 4000 Events](#) Selected 0 / Total 1

Troubleshoot Upload New Mibs Show Quick Filter

Description  
flapping

☐ Port 'GigabitEthernet0/3/0/19' is flapping on device '10.126.165.17'.

General Information

Event Type	Link up
Event Source	10.126.165.17
Event Category	Routers
Change Last Detected	September 11, 2015 5:30:13 AM IST
Device IP Address	10.126.165.17
Severity	<span style="color: red;">✖</span> Critical

406010

## Which Events Are Supported?

Refer to the following documents for information on the events that are supported by Cisco EPN Manager .

- [Cisco Evolved Programmable Network Manager Supported Traps](#)
- [Cisco Evolved Programmable Network Manager Supported Syslogs](#)
- [Cisco Evolved Programmable Network Manager Supported TL1 Messages](#)


For information about how unsupported events are handled, see [View Events \(Including Generic Events\)](#), on page 230.

## Set Alarm and Event Management Preferences

- [Set Up Your Alarm and Event Display Preferences](#), on page 218
- [Customize the Alarm Summary](#), on page 220




### Note

Advanced users can also use the Cisco EPN Manager Representational State Transfer (REST) API to access device fault information. For information on the API, click  at the top right of the Cisco EPN Manager window and choose **Help > API Help**.



## Set Up Your Alarm and Event Display Preferences

In the Alarms and Events tables, Cisco EPN Manager displays the last 4000 alarms or events, by default. Cisco EPN Manager can only display what is available in the cache (which may be less than 4000). If you want to see more than 4000 alarms or events, click **Show All** above the table.

You can customize the following alarm and event display by clicking  at the top right of the Cisco EPN Manager window and choosing **My Preferences**. After you make your changes, click **Save** to apply your new settings. Other settings, such as whether acknowledged, cleared, and assigned alarms are displayed, are controlled globally by the administrator. (see [Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms](#), on page 708).

User Preference Setting	Description
<b>Automatically refresh Alarms &amp; Events page</b>	Enables or disables automatically refreshing of the Alarms and Events page. If enabled, the page is refreshed according to the setting in <b>Refresh Alarm count in the Alarm Summary</b> .
<b>Refresh Alarm count in the Alarm Summary every ____ minutes/seconds</b>	Sets the refresh interval for the alarm count in the Alarm Summary (1 minutes by default) (see <a href="#">Customize the Alarm Summary</a> , on page 220).
<b>Enable Alarm Badging on Alarms &amp; Events page</b>	When user enables Alarm Badging, alarm severity icons are displayed next to the device groups on the <b>Monitor &gt; Monitoring Tools &gt; Alarms &amp; Events</b> page.
<b>Disable Alarm Acknowledge Warning Message</b>	<p><b>Note</b> This setting is only configurable if <b>Hide Acknowledged Alarms</b> is also enabled; that setting is disabled by default (see the previous table).</p> <p>Disables the following message from displaying when user selects an alarm and chooses <b>Change Status &gt; Acknowledge</b>:</p> <p><b>Warning: This alarm will not be generated, if the original event recurs again, within next 7 days, as it is acknowledged now. Clearing the alarm instead of acknowledging will cause the alarm to be generated if the event recurs again. Proceed with alarm acknowledgment?</b></p>
<b>Disable confirmation prompt for “Clear all of this condition”</b>	<p>Disables the following message from displaying when user selects an alarm and chooses <b>Change Status &gt; Clear all of this condition</b>:</p> <p><b>Are you sure you want to clear all alarms of this condition?</b></p> <p>(Disabled by default)</p>



User Preference Setting	Description
<b>Disable “Set severity to information” prompt for “Clear all of this condition”</b>	<p>Disables the following message which is displayed when user selects an alarm and chooses <b>Change Status &gt; Clear all of this condition</b>:</p> <p><b>Do you want to set the severity for the selected alarm's condition to Information?</b></p> <p><b>WARNING: This is a system-wide change that will prevent creation of future alarms of this condition. You can undo this change on the Severity Configuration page under System Settings.</b></p> <p>(Disabled by default)</p> <p><b>Note</b> Users with sufficient privileges can reset the severity to its original value using the procedure in <a href="#">Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms</a>, on page 708.</p>
<b>Select alarm categories for Alarm Summary Toolbar</b>	Controls what is displayed in the Alarm Summary (see <a href="#">Customize the Alarm Summary</a> , on page 220).
<b>When clearing all alarms of a condition, always set the condition's severity to Information</b>	When user selects an alarm and chooses <b>Change Status &gt; Clear all of this condition</b> . (Disabled by default)
<b>Enable New Critical Alarm Count Notifications</b>	Enables the notification pop-up that displays the count of critical alarms. The count gets updated once the alarm interval is refreshed depending on the interval set in <b>Refresh Alarm count in the Alarm Summary</b> (see <a href="#">Customize the Alarm Summary</a> , on page 220). Only the outstanding critical alarms are displayed.

## View Critical Alarm Notifications

The count of the critical alarms in the network is displayed as a notification pop-up in every page. The count gets refreshed every 1 minute or some interval depending on the interval set in the **My Preferences** page.

The screenshot shows the Evolved Programmable Network Manager interface. At the top, there is a navigation bar with the title "Evolved Programmable Network Manager" and a search bar. Below the navigation bar, the breadcrumb path is "Managed Elements / Network Devices". The main content area displays a table of network devices. The table has columns for "Reachability", "Admin Status", "Device Name", "IP Address", "DNS Name", "Device Type", and "Last Inventory Collection". The first four rows of the table show devices with "Managed" status and "Completed" collection status. A notification pop-up in the top right corner indicates "2 new critical alarm in Show Details Total 22".

Reachability	Admin Status	Device Name	IP Address	DNS Name	Device Type	Last Inventory Collection
<input checked="" type="checkbox"/>	Managed	ASR9001-127.156.cisco	10.127.101.156	10.127.101.156	Cisco ASR 9001 Router	Completed
<input checked="" type="checkbox"/>	Managed	ASR903-101.110.cisco	10.127.101.110	10.127.101.110	Cisco ASR 903 Router	Completed
<input checked="" type="checkbox"/>	Managed	ASR903-101.112.cisco	10.127.101.112	10.127.101.112	Cisco ASR 903 Router	Partial Collection Failure
<input checked="" type="checkbox"/>	Managed	ASR920-101.114.cisco	10.127.101.114	10.127.101.114	Cisco ASR920 12 CZA Ro...	Completed

Click the **Show Details** hyperlink to view the list of critical alarms in the **Monitor > Monitoring Tools > Alarms and Events > Alarms** page.



**Note** Only the outstanding critical alarms are taken count and displayed.

The notification is not enabled by default and needs to be enabled from the **My Preferences** page. For details on how to enable the critical alarm count notification, see [Set Up Your Alarm and Event Display Preferences](#), on page 218.

## Customize the Alarm Summary


You can specify what alarm categories are displayed:

- In the Cisco EPN Manager title bar alarm count (bell). This gives you a quick visual count of alarms you are interested in.
- In the Alarm Summary pop-up window that is launched when you click the alarm count. The pop-up window gives you a quick look at alarm counts with their severity, as shown in the following figure.

Category	Critical	Major	Minor
<b>Alarm Summary</b>	<b>20</b>	<b>42</b>	<b>115</b>
Application Performance	0	0	0
Autonomous AP	0	0	0
BGP	0	4	2
Carrier Ethernet	0	5	27
Cisco Interfaces and Modules	0	0	0
Cisco UCS Series	0	0	0
MPLS	0	0	0
MPLS-L3VPN	0	2	0
Optical Transport	17	21	77
OSPF	0	4	2
Performance	0	0	0
Routers	3	5	5
Security	0	0	0

Last Updated: Wednesday, September 16 2015, 11:43 AM [View Details](#)

To customize this information:

- Step 1** Click **Edit** at the top left of the Alarm Summary pop-up window. This opens your My Preferences page. You can also open this page by clicking  at the top right of web GUI window and choosing **My Preferences**.
- Step 2** Go to the **Alarms** area.
- Step 3** To change the Alarm Summary refresh interval, select a number from the **Refresh Alarm count in the Alarm Summary every** drop-down list.
- Step 4** To specify what is included in the Alarm Summary, next to **Select alarms for Alarm Summary Toolbar**, click **Edit Alarm Categories**. This opens the Select Alarm Categories dialog box.

To change:	Do the following:
Alarm count displayed in the web GUI title bar	From the <b>Default Category to display</b> drop-down list, choose the categories you want to include in the alarm count.
Alarm types listed in the Alarm Summary pop-up window	Under the <b>Show</b> drop-down, check each alarm category or sub-category you want to see listed in the Alarm Summary pop-up window. If you want to include most alarms, check the <b>Alarm Category/Subcategory</b> check box, then uncheck the alarms you do not want to include.








**Step 5** Click **OK** in the Select Alarm Categories dialog box, then click **Save** in the My Preferences window.

## Interpret Event and Alarm Badges and Colors

When there is a problem in the network, Cisco EPN Manager flags the problem by displaying an alarm or event icon with the element that is experiencing the problem. [Alarm Severity Icons, on page 221](#) lists the icons and their colors.

### Alarm Severity Icons

The table below lists the alarm colors and their respective severity levels for the icons displayed in various parts of the web GUI.

Severity Icon	Description	Color
	Critical alarm	Red
	Major alarm	Orange
	Minor alarm	Yellow
	Warning alarm	Light Blue
	Alarm cleared; normal, OK	Green
	Informational alarm	Medium Blue
	Indeterminate alarm	Dark Blue

## Find and View Alarms

To view alarms, go to **Monitor > Monitoring Tools > Alarms and Events**. From the displayed alarms table, you can search for specific alarms, as described in the table below. You can also create and save customized

(preset) filters as described in the procedure that follows the table. To get more information about an alarm, see [View an Alarm's Details](#), on page 225.

**Note**

By default, acknowledged and cleared alarms are not included for any search criteria. This behavior is controlled by the system administrator. See [Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms](#), on page 708

To find these alarms:	Choose <b>Monitor &gt; Monitoring Tools &gt; Alarms and Events</b> and:
Alarms generated by specific device	<p>For active alarms, click the “i” icon next to the device name to open the Device 360 view, then click the <b>Alarms</b> tab. For cleared alarms, refer to the Alarms and Events table.</p> <p>For cleared alarms or correlated alarms, click the appropriate tab and enter the device name or component in the <b>Location</b> column. You can use wild cards.</p> <p>For certain devices, you can also use the Chassis View to check device alarms. See <a href="#">View Alarms in the Chassis View</a>, on page 80.</p>
Alarms generated by a specific circuit/VC	<ol style="list-style-type: none"> <li>1. Click the “i” icon next to the device name to open the Device 360 view, then click the <b>Circuit/VC</b> tab.</li> <li>2. Click the “i” icon next to the Circuit/VC name to open the Circuit/VC 360 view, then click the <b>Alarms</b> tab.</li> </ol> <p>See <a href="#">Check Circuits/VCS for Faults</a>, on page 551 for information on other ways to get circuit/VC alarm information.</p>
All alarms in the network	Click the <b>Show All</b> link.
Alarms assigned to you	Click the <b>Show</b> drop-down filter list and choose <b>Alarms assigned to me</b> . You can also use this filter for cleared and correlated alarms.
Unassigned alarms	Click the <b>Show</b> drop-down filter list and choose <b>Unassigned Alarms</b> . You can also use this filter for cleared and correlated alarms.
Latest alarms according to the Cisco EPN Manager timestamp	<p>For active alarms:</p> <ul style="list-style-type: none"> <li>• Alarms in the last 30 minutes—Click the Show drop-down filter and choose the last 5, 15, or 30 minutes (<b>CEPNM timestamp</b>).</li> <li>• Alarms in the last 24 hours—Click the Show drop-down filter and choose the last 1, 8, or 24 hours (<b>CEPNM timestamp</b>).</li> <li>• Alarms in the last 7 days—Click the Show drop-down filter and choose the last 7 days (<b>CEPNM timestamp</b>).</li> </ul> <p>You can use these same filters for cleared and correlated alarms. The filters do not have the (<b>CEPNM timestamp</b>) suffix because filtering by device timestamps is not supported for cleared and correlated alarms. For more information on (<b>CEPNM timestamp</b>) and (<b>Device timestamp</b>), see <a href="#">Device Timestamp and CEPNM Timestamp</a>, on page 223.</p>

To find these alarms:	Choose Monitor > Monitoring Tools > Alarms and Events and:
Latest alarms according to the device timestamp	Follow the same instructions as in the previous row, but choose the filters with the suffix <b>(Device timestamp)</b> This filter is not supported when searching for cleared or correlated alarms.
All alarms generated by a device group, series, or type	Choose a group from the navigation pane on the left. You can also use this filter for cleared and correlated alarms.
Alarms using customized filters	Create and save the advanced filter (see the procedure that follows this table).

You can also filter the data to find specific alarms using a *quick filter* or an *advanced filter* from the **Show** drop-down list. For information about how to filter the data, see [Filter Data in the Detailed Tables, on page 153](#).

## Device Timestamp and CEPNM Timestamp

While **Device timestamp** is the information embedded inside the syslogs message, **CEPNM timestamp** is the time at which that message from the device is received at Cisco EPN Manager end.

The following configuration is recommended on the device:

**service timestamps log datetime show-timezone msec year**

Note that these are the default formats supported in case of a Device timestamp:

- yyyy MMM dd HH:mm:ss.SSS z
- yyyy MMM dd HH:mm:ss z
- MMM dd HH:mm:ss z
- yyyy MMM dd HH:mm:ss.SSS
- yyyy MMM dd HH:mm:ss
- MMM dd HH:mm:ss

Where **z** in the format implies a time zone.



**Note** Only 3 letter time zones are supported and time zones with hour/minute offsets are not supported.

## View a Specific Alarm in the Topology Map

From the Alarms table, you can select a specific alarm and launch the topology map to see the alarm on the map.

**Step 1** To display the Alarms table, choose **Monitor > Monitoring Tools > Alarms and Events**.

**Step 2** In the Alarms tab, locate and select the required alarm.

**Step 3** Choose **Troubleshoot > Network Topology**.

The view switches to the topology map and the device with the alarm is highlighted in the map.

## View Root Cause and Correlated Alarms

The Cisco EPN Manager correlation process determines the causality for alarms and alarm sequences. Alarms that support the correlation process can be:

- A root cause alarm—An alarm that causes other alarms (the "correlating" alarm).
- A symptom alarm—An alarm that is the result of another alarm (the "correlated to" alarm).

Root cause and symptom alarms are displayed in a hierarchical manner to help you easily identify impacted network elements. The following is an example of an uncleared link down alarm that is the root cause for two other link down symptom alarms. To display an alarm tooltip in the hierarchy, hover your mouse over an alarm.

Contained Alarms for ASR903-101.110 : Port 'GigabitEthernet0/3/1' (Description: ' "Connected to CE - 144 "') is down on device '10.255.101.110'.

Severity	Message	Failure Source	Timestamp	Category	Condition	Location
Critical	Port 'GigabitEthernet0/3/1' is down on device '10.255.101.110'.	ASR903-101.110	8 June, 2016 12:25:47 P...	Routers	Link down	GigabitEt...
Major	mplsL3VpnVrfDown...	ASR903-101.110	8 June, 2016 12:25:45 P...	MPLS-L3VPN	mplsL3VpnVrf...	CUST1
Warning	cVrftDown on Dev...	ASR903-101.110	8 June, 2016 12:25:44 P...	MPLS-L3VPN	cVrftDown	GigabitEt...

This view is especially helpful when alarm sequence has multiple hierarchies. All alarm sequences, regardless of the number of hierarchies, have only one root cause alarm.

**Step 1** Choose **Monitor > Alarms and Events**.

**Step 2** To view *uncleared* correlated alarms, click the **Correlated Alarms** tab.

You can also view uncleared correlated alarms in the main Alarms and Events table. The **Correlation Type** column will identify whether it is an uncleared root cause alarms or symptom alarm (with a hyperlink to more information).

*Cleared* correlated alarms are displayed in the **Cleared Alarms** tab. Like uncleared alarms, the **Correlation Type** column will identify it as a cleared root cause or symptom alarm.

# Get Troubleshooting and Detailed Alarm Information

- [View an Alarm's Details, on page 225](#)
- [Find Troubleshooting Information for an Active Alarm, on page 225](#)
- [Find Out Which Events Are Associated With An Alarm, on page 226](#)
- [Find Out If An Alarm Impacts Other Services or Network Elements, on page 226](#)

## View an Alarm's Details

To get more details about an alarm, expand it. You can do this from the Alarms list (by choosing **Monitor > Monitoring Tools > Alarms and Events**, or by clicking **Details** in the Alarm Summary pop-up). The circled areas are explained in the table that follows this figure.

The screenshot displays the 'Details' view for a specific alarm. At the top, a table lists the alarm's severity (Major), message, status (Not Acknowledged), failure source, timestamp, owner, category (Routers), and condition (Pseudowire tunnel down). Below this, the interface is organized into five main sections, each with a red circle highlighting its title:

- General Information:** Displays metadata about the alarm, including Source (10.56.23.16), Acknowledged status (No), Category (Routers), Alarm Found At (February 25, 2015 4:40:57 AM EST), Alarm Last Updated At (February 25, 2015 7:17:50 AM EST), Alarm Detected Through (Carrier Ethernet), Severity (Major), and Previous Severity (Major).
- Device Details:** Provides information about the device associated with the alarm, including IP Address (10.56.23.16), Device Name (ASR901-CSG-1-DOMAIN1.cisco.com), Device Type (Cisco ASR 901 100 Series Aggregation Services Routers), Up Time (17 days 16 hrs 20 mins 7 secs), Reachability Status (Reachable), Collection Status (Managed with Errors), Software Version (15.4(3)B), Serial Number (CAT1651U0SL), Location, and Contact.
- Messages:** Shows the message text: 'Device ASR901-CSG-1-DOMAIN1.cisco.com: Pseudowire tunnel with Local IP 50.1.20.23, PwId 112, and Remote IP 8.8.8.8 is down'.
- Impacted Circuits/VCs:** Displays a table of circuits affected by the alarm. The table has columns for Alarms, Name, Type, Date Created, Last Modified, Custome..., Status, and Sta. One entry is visible: EvcLink\_E... (EVC) created on February 24, 2015, with status Discov... and Disco.
- Device Events:** Shows a table of recent device events. The table has columns for Severity, Description, Source, and Timestamp. The message 'No data available' is displayed.

<b>General Information</b> —When alarm was found and last updated, current and last severity, and how it was detected	<b>Device Details</b> —Managed device name, address, uptime, reachability status, collection status, and so forth
<b>Messages</b> —Trap, syslog, or TL1 message	<b>Device Events</b> —Recent device events from past hour (of any type, in chronological order)
<b>Impacted Circuits/VCs</b> —Carrier Ethernet or Optical circuits/VCs affected by alarm	

## Find Troubleshooting Information for an Active Alarm

Use this procedure to get an explanation for why an active alarm occurred, and the recommended response to the alarm.



**Note** Not all alarms have this information. Users with sufficient privileges can add or change the information that is displayed in the popup window. See [Customize the Troubleshooting Text for an Alarm](#), on page 710.

**Step 1** Choose **Monitor > Monitoring Tools > Alarms and Events**, then click the **Alarms** tab. (For interface alarms, you can also get this information from the Interface 360 view under the **Alarms** tab.)

**Step 2** Locate the alarm, then click the "i" icon in the **Condition** column to open the popup window that provides the explanation and the recommended action that can be taken to troubleshoot the alarm.

If you take any actions, we recommend you document your actions. Choose the alarm, click **Annotation**.

## Find Out Which Events Are Associated With An Alarm

To view the events that have been correlated to an alarm, from the Alarms table, click the "i" icon next to the Severity.

The screenshot shows a list of alarms on the left and a popup window titled "Most Recent Events for Routers Alarm:". The popup window contains a table with the following data:

Description	Source	Time
Device 'ASR901-C'.Pseudowire tunnel...	ASR901-C...	February 25, 2015 12:32:33 PM EST
Device 'ASR901-C'.Pseudowire tunnel...	ASR901-C...	February 25, 2015 12:32:25 PM EST
Device 'ASR901-C'.Pseudowire tunnel...	ASR901-C...	February 25, 2015 12:32:21 PM EST

Below the table, there is an "Actions" section with a link: "All Events in Last 8 Hours".

## Find Out If An Alarm Impacts Other Services or Network Elements

The Alarms table contains a **Service Affecting** column which tells you if an alarm affects other parts of the network:



**Note** Service-affecting information is displayed for optical devices only.

- SA means it is a service-affecting alarm
- NSA means it is not a service-affecting alarm

To identify all alarms that can affect services, choose **Quick Filter** from the Show drop-down list and enter **SA** in the field above the Service Affecting column.

To find out which services are affected, expand the alarm and check the details in the Impacted Circuits/VCs area of the alarm details.



The Alarms table also contains a **Correlation Type** column which tells you if the alarm is causing other alarms (Root Cause Alarm), or if the alarm is a symptom of another alarm (Symptom Alarm). For more information, see [View Root Cause and Correlated Alarms, on page 224](#).

## Acknowledge and Clear Alarms

An alarm can have a status of Not Acknowledged, Acknowledged, or Cleared.

### Not Acknowledged

Not Acknowledged means the problem is not being worked on. It could indicate that a new fault condition in the network, or that a cleared fault condition that has recurred. Not Acknowledged alarms are not removed from the Alarms and Events tables until they are either acknowledged or cleared.

### Acknowledged

Acknowledged means a fault condition has either been recognized and is being worked on, or it can be ignored. Moving an alarm to the acknowledged status is a manual operation and changes the alarm Status to Acknowledged. An acknowledged event is still considered to be open (that is, not cleared), so if any related events recur, the events are added to the alarm.

By default, acknowledged alarms are not removed from the Alarms list. This behavior depends on the **Hide Acknowledge Alarms** setting that is controlled by the Administrator.

Acknowledged alarms can be moved back to the Not Acknowledged status (for example, if you acknowledged the wrong alarm).

### Cleared

Cleared means the fault condition no longer exists. If an alarm is cleared but an associated event recurs, Cisco EPN Manager opens a new alarm. An alarm can be cleared by a user or by the Cisco EPN Manager system. Cleared alarms are removed from the Alarms list (but you can still view them under the Cleared Alarms tab).

You can also clear an alarm by choosing **Clear all of this Condition**, which will clear all alarms that are having the same problem. You may also be prompted to change all alarms with that condition to Informational severity. This means that if an associated event recurs, a new alarm will *not* be opened. You should use that setting with care.

To change the status of an alarm:

---

**Step 1** Choose **Monitor > Monitoring Tools > Alarms & Events**.

**Step 2** Select an alarm, then choose **Change Status** and the appropriate status (Acknowledge, Unacknowledge, Clear, Clear all of this Condition).

**Note** **Clear all of this Condition** triggers a clearing event for *all alarms* with the same condition as the alarm you selected. When you choose this status, Cisco EPN Manager displays a dialog asking if you want to change the severity for the selected alarm condition to Information. This prevents Cisco EPN Manager from issuing alarms for the specified condition. To later reset the condition's severity, choose **Administration > System Settings > Severity Configuration** and modify the severity. See [Change Event Severity Levels, on page 709](#) for more information.

**Step 3** Click **Yes** to confirm that you want to clear all alarms of the specified condition.

## What are the Supported Alarm Clearing Mechanisms

At times you may face a situation where there are so many alarms that are available irrespective of their events being cleared. If you encounter any such problems, here are some of the solutions supported in Cisco EPN Manager .

- **Default clearing of alarms**—The fault is resolved on the device and an event is triggered for the same. For example, a device-reachable event clears the device-unreachable event. This in-turn, clears the device-unreachable alarm.
- **Auto-clearing of alarms**—In some cases, a device may not generate a clearing alarm. In such cases, Cisco EPN Manager waits for 24 hours (default interval) and then auto-clears the alarm. You need to have administrator privileges to change the auto-clear duration and to know how to set that interval, see [Change Alarm Auto-Clear Intervals, on page 710](#) .
- **Clearing alarms based on inventory status of ports**—When a device is rebooted, a card is reloaded or a RSP failover happens, the inventory collection is triggered for that device. During this inventory synchronisation, Cisco EPN Manager clears several types of alarms located on some specific ports based on the operational status of that particular port of the device. For example, when Cisco EPN Manager receives a Link Down trap from a device, it generates a Link Down alarm on the specific port since it is operationally down. After a device reboot, if the operational status of the port changes to up, then the Link Down alarm is cleared automatically by Cisco EPN Manager .
- **Syncing device to clear alarms**—Here, the devices are synced so that Cisco EPN Manager gets the list of the outstanding active alarms and the events that does not exist are cleared. This is a different mechanism when compared to the event based alarm/event reporting (over traps/syslogs). Once the sync is over, the Alarms Table is refreshed to display only the outstanding active alarms.



**Note** This feature is supported only for certain devices or for certain device functionalities. For example, this feature is supported for optical devices/optical part of devices (For example, NCS 4K, NCS 1K) and is not supported for packet devices (For example, ASR 9K, 9xx, 42xx, 4K).

- **Manual clearing of alarms**—In situations where the clearing event is missing, you can manually clear an alarm by choosing the particular alarm, and changing its status to Clear. For more information, see the **Cleared** section under [Acknowledge and Clear Alarms, on page 227](#).

## Add Notes To an Alarm

The annotation feature allows you to add free-form text to the alarm, which is displayed in the Messages area of the alarm details. To add text to an alarm, choose the alarm in the Alarms and Events table, click **Annotation**,

and enter your text. As with acknowledging, when you annotate an alarm, Cisco EPN Manager adds your user name and the annotation time stamp to the Messages area of the alarm details.

## Forward Alarms and Events as Email Notifications

You can configure Cisco EPN Manager to send email notifications for alarms and events. You can specify the severity for which you want to be notified, and the notification email destinations. The settings for the email subject line and body of the email are controlled globally by the administrator; you cannot adjust them.

- 
- Step 1** Choose **Monitor > Monitoring Tools > Alarms and Events**.
- Step 2** Click **Email Notification**.
- Step 3** Configure the email notification contents.
- In the **Enable** column, select the check box for the alarm you want to include in the notification.
  - Click the alarm name hyperlink and do the following:
    - Select the severity levels for which you want a notification to be sent.
    - Enter the email addresses in the **To** field.
- Step 4** Click **Save**.
- 

## Manage How Alarms are Triggered (Alarm Thresholds)

You can customize how often information is gathered (polling interval), the threshold value that indicates a problem, and whether Cisco EPN Manager should generate an informational event or an alarm (of an severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

- 
- Step 1** Choose **Monitor > Monitoring Tools > Monitoring Policies > My Policies** and select the policy you want to edit.
- Step 2** Locate the parameter you want to change. You can search for the parameter by entering a string in the **Parameter** text box.
- Step 3** To adjust the polling interval, select the new interval from the **Polling Frequency** drop-down list. To disable polling, choose **No Polling**. Note that some polling frequencies are applied to groups of parameters. Changing the group interval will change the polling for all settings in the group. If a policy does not have any thresholds or events associated with it, Cisco EPN Manager prompts you to save the changes.
- Step 4** To change a threshold value, expand the parameter and choose a value from the parameter's drop-down list.
- Step 5** To specify what Cisco EPN Manager should do when the threshold is surpassed, choose an alarm value from the parameter's drop-down list. You can configure Cisco EPN Manager to generate an alarm of a specified severity, generate an informational event, or do nothing (if no reaction is configured).
- Step 6** Click:
- Save and Activate** to save and activate the policy immediately on the selected devices.

- **Save and Close** to save the policy and activate it at a later time.

## View Events (Including Generic Events)

The Events tab displays supported and generic (unsupported) events. Supported events are events that Cisco EPN Manager generates based on information about the network. It receives this network information either through syslogs and traps generated by devices, or through polling and inventory collection. This process is described in [How are Alarms and Events Created and Updated?](#), on page 214. Generic events are events that Cisco EPN Manager does not recognize. Rather than drop the events, Cisco EPN Manager assigns the events a Minor severity (this severity is applied to all generic events; to change it, see [Change Event Severity Levels](#), on page 709). If desired, you can customize the information displayed by generic events; see [Customize Generic Events That Are Displayed in the Web GUI](#), on page 712. For information about supported events, see [Which Events Are Supported?](#), on page 217.

Generic event processing is disabled by default. Users with Administrator privileges can disable or re-enable it.

The Events tab provides a variety of filters that you can use to find the information you are looking for. You can also create and save customized (preset) filters using the same procedure described in [Find and View Alarms](#), on page 221. The following table lists some of the ways you can filter events.



To find these events:	Select Monitor > Monitoring Tools > Alarms and Events, click the Events tab, and:
All events in the network	Click the <b>Show All</b> hyperlink
Latest 4,000 Events	Click the <b>Show Latest 4000 Events</b> hyperlink
All events generated by a device group, series, type, location group, or user-defined group	Choose a group from the left sidebar menu
Events in last <i>x</i> minutes, hours, or days	Click the <b>Show</b> drop-down filter list and choose the appropriate filter
Non-informational events generated in the last hour	From the <b>Show</b> drop-down filter list, choose <b>Non-info events in last hour</b>
Events using customized filters	Create and save an advanced filter (see <a href="#">Find and View Alarms</a> , on page 221)

## View Syslogs (Historic)

Cisco EPN Manager logs all syslogs from severity 0 through 7 (emergency through debugging messages) generated by all devices that are managed by Cisco EPN Manager. Syslogs from devices that are not managed are not logged or displayed. Cisco EPN Manager also logs all SNMP messages.

Cisco EPN Manager stores a maximum of 2,000,000 syslogs with the following display limits:

- Live syslog streaming—Latest 2,000 syslogs. For more information on live syslogs, see [View Live Syslogs, on page 231](#).
- Historic syslogs—Maximum of 200,000 syslogs.

- 
- Step 1** Choose **Monitor > Monitoring Tools > Alarms and Events**. Click the **Syslogs** tab.  
You can also view the historic syslogs in the **Historic** tab in **Monitor > Monitoring Tools > Syslog Viewer**.
- Step 2** Click **Custom Syslog Events** to enable Cisco EPN Manager to create events for particular syslogs. You can specify a syslog message identifier, event severity and message to use when the specified syslog is received. Cisco EPN Manager creates an event with the settings you specify.  
Also, if there is an existing syslog for which you want to create an event, select the syslog, then click **Custom Syslog Events**.
- Step 3** Click **Add**. Complete the required fields. If you selected an existing syslog in Step 2, the Message Type and Event Message fields are pre-populated with the values of the syslog you selected.  
You can edit or delete the customized event that was created.
- Step 4** Select a **Default Severity** level, then click **OK**. The Default Severity field controls the severity of the event that is created from the syslog. The syslog itself is not modified in any way.
- Step 5** To export the syslogs to a CSV, click  at the top right of the table/page on the particular syslog tab to open the **Export** dialog box.
- Step 6** Click **Export**. The first 100000 records will be exported.
- Step 7** Click  to open a Support Case. See [Open a Cisco Support Case, on page 714](#).
- 

## View Live Syslogs



Cisco EPN Manager displays the live streaming of syslogs in **Monitor > Monitoring Tools > Syslog Viewer**.



**Note** However, this view is not recommended as it has a limitation of only 10 devices. Instead, you can view syslogs (historic) in the **Syslogs** tab in **Monitor > Monitoring Tools > Alarms and Events**. See [View Syslogs \(Historic\), on page 230](#).

---



- 
- Step 1** Choose **Live** tab in the Syslog Viewer page.
- Step 2** Use the filters to locate different syslogs. You can enter regular expressions in the fields; for example: `^Auth, V|violation|$, ^Sec*V|violation$`
- Step 3** If the data is excessive, click the Pause icon. You can click the Resume arrow at any time.
- Step 4** If you do not want to see duplicates of a syslog, click **De-duplicate**. Cisco EPN Manager will aggregate the syslogs of that type into one line item and display the count in the **Count** field.

- Step 5** To view older syslogs (syslogs that were received before you clicked the **Live** tab), click the **Historic** tab. See [View Syslogs \(Historic\)](#), on page 230.
- Step 6** To export the live syslogs to a CSV, click  at the top right of the table/page on the particular syslog tab to open the **Export** dialog box.
- Step 7** Click **Export**. The first 100000 records will be exported.
- Step 8** Click  to open a Support Case. See [Open a Cisco Support Case](#), on page 714.
- 

## Export Alarms or Events to a CSV or PDF File

Use this procedure to save alarms or events as a CSV or PDF file.

---

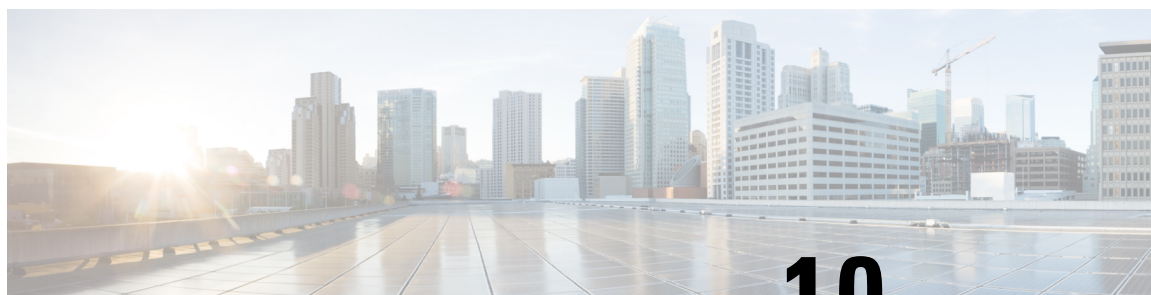
- Step 1** Navigate to the data you want to export.
- Alarms—Choose **Monitor > Monitoring Tools > Alarms and Events**, then click the **Alarms** or **Cleared Alarms** tab.
  - Events—Choose **Monitor > Monitoring Tools > Alarms and Events**, then click the **Events** tab.
- Step 2** If you have a very large amount of data, apply a filter; otherwise the export process may take some time.
- Step 3** Click  at the top right of the table to open the **Export** dialog box.
- Step 4** Choose CSV or PDF, click **OK**, and save the file.
- To export the events for a particular alarm, in the **Alarms** tab, hover the mouse over the "i" icon next to the particular alarm. In the pop-up window that opens, click  at the top right corner to perform the export operation.
- 

## Get Support from Cisco

If you receive an alarm in **Monitor > Monitoring Tools > Alarms and Events** for which you cannot find a resolution in the Cisco Support Community (click an alarm, then choose **Troubleshoot > Support Forum**), you can use Cisco EPN Manager to open a support request (click an alarm, then choose **Troubleshoot > Support Case**).

## Respond to Problems Within Cisco EPN Manager

Cisco EPN Manager generates internal SNMP traps to monitor its own functions—such as server CPU and disk utilization, fan and power supply failures, and high availability (HA) state changes. For information on these types of events, see [Troubleshoot Server Internal SNMP Traps](#), on page 653.



## CHAPTER 10

# Monitor Cisco ASR 9000 Network Virtualization (nV) Satellites and Cluster Services

- [Monitor Cisco ASR 9000 nV Satellites, on page 233](#)
- [Monitor a Cisco ASR 9000 nV Edge Cluster, on page 241](#)

## Monitor Cisco ASR 9000 nV Satellites

- [Minimum Device and OS Requirements for Cisco ASR 9000 nV Satellites, on page 235](#)
- [View Cisco ASR 9000 Host-Satellite Topologies in the Topology Map, on page 235](#)
- [Identify the Satellites Connected to a Cisco ASR 9000 Host, on page 236](#)
- [Identify the Hosts Connected to a Satellite, on page 238](#)
- [Monitor Cisco ASR 9000 nV Satellites for Faults, on page 238](#)

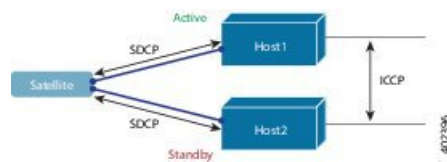
The Cisco ASR 9000 nV satellite feature set allows one or more smaller satellite switches to be interconnected with an Cisco ASR9000 device to form a single, combined access, aggregation and edge system.

Cisco EPN Manager supports Cisco ASR 9000v, Cisco ASR 901, Cisco ASR 901S and Cisco ASR 903 devices as satellites. The Cisco ASR 9000v is a dedicated satellite switch that can only be used in nV satellite mode along with an Cisco ASR 9000 device. The Cisco ASR 901 and Cisco ASR 903 switches are “dual mode” switches. This means that they can operate both as standalone switches or as satellite switches within an nV system with an Cisco ASR 9000 device (in which case they are completely managed and controlled by the master Cisco ASR 9000).

The satellite feature allows for both redundant and non redundant interconnections between the satellite switches and the master Cisco ASR 9000s. The access side Ethernet ports of the satellite switches appear within the control and management planes of the host master Cisco ASR 9000 just like locally connected Ethernet ports. All features that can be configured on the host Cisco ASR 9000 can also be configured and executed identically on satellite located ports. Effectively the satellite switches are *virtual line cards* of the host Cisco ASR 9000. Chassis management functions of the satellites such as software upgrades, inventory and environmental monitoring of hardware sensors (voltage, temperature etc) on the satellites are also seamlessly integrated into the same functions of the host Cisco ASR 9000, just like any other line card of the host Cisco ASR 9000 chassis.

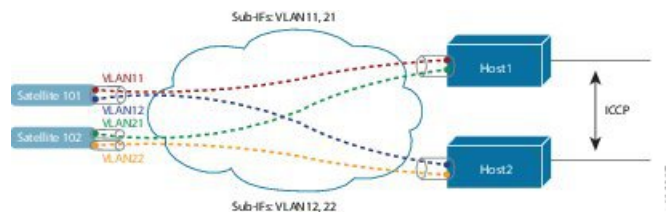
Cisco EPN Manager supports the following types of nV Satellite configurations:

- Dual home hub and spoke (inventory support only)



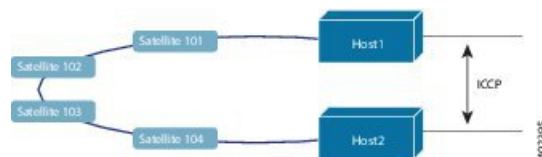
- The same satellite is dual homed to two separate Cisco ASR 9000 hosts – active and standby.
- Each host has an independent control channel with the satellite.
- The satellite is notified which host is active and which is standby.
- If the satellite loses its active host or link, failover occurs to its standby host.

#### • L2 fabric hub and spoke



- L2 Fabric supports satellite connectivity across Ethernet Layer 2 domains.
- Satellite Fabric Link Redundancy—single physical link with two VLANs/EVCs or two physical links with one VLAN/EVC each.
- Each host L2 sub-interface is mapped to one satellite fabric port.

#### • Simple Ring



- Each satellite in the ring runs SDCP with two hosts independently.
- Each satellite maintains a logical hub-and-spoke topology over the physical ring topology.
- No local switching directly between satellites - all packets traverse the host.

## Satellite Considerations in Cisco EPN Manager

Satellites are not displayed in the Network Discovery page (**Inventory > Device Management > Network Devices**) because Cisco EPN Manager does not support satellite device management operations from that page.

Satellites can only belong to Location groups because, as network nodes, they are normally managed according to location. In addition, if you add a host device to a group, its satellites are not automatically added to the group unless the group meets the following guidelines.

- If you use Add Devices Manually—From the create (or edit) group page, click Add, then choose All Locations from the Filter by drop-down list. The satellites will be listed if they match your criteria.
- If you use Add Devices Dynamically—Make sure you are creating a location group; and from the create (or edit) group page, choose All Locations from the Parent Group at the top of the page.



## Minimum Device and OS Requirements for Cisco ASR 9000 nV Satellites

The following are the minimum device and device operating system requirements for the nV satellite feature set.

- Hardware — Cisco ASR 9000 Series Aggregation Services Routers with Cisco ASR 9000 Enhanced Ethernet line cards as the location of Inter Chassis Links and Cisco ASR9000v, Cisco ASR 901, Cisco ASR 903, Cisco NCS 5001, or Cisco NCS 5002 routers as satellite devices.
- Software — Cisco IOS XR 5.2.0.

Additional support may be available. For more information see the [Cisco Evolved Programmable Network Manager Supported Devices](#).

## Get Quick Information About a Specific Satellite: Satellite 360 View

The Satellite 360 view is a popup window that provides quick information about a satellite device, its inventory, and its status. This includes device alarms, modules, interfaces, and hosts.

To launch a Satellite 360 view:

- Click the "i" icon next to the device name in almost any device table
- From the network topology, click a device in an expanded group, then click **View**
- 

The Satellite 360 view provides general satellite device information at the top of the view, and more detailed interface information in tabs in the lower part of the view.

Information Provided in Satellite 360 View	Description
General information	The satellite device type and name, status, last configuration change, and last inventory collection,
Modules	Modules that are configured on the satellite device, including their name, type, state, ports, and location.
Interfaces	Name, operational and admin status for each associated satellite device . Also provide a launch point for the Interface 360 view.
Hosts	Name, IP address, and role (Active or Standby) of host devices that are connected to the satellite.

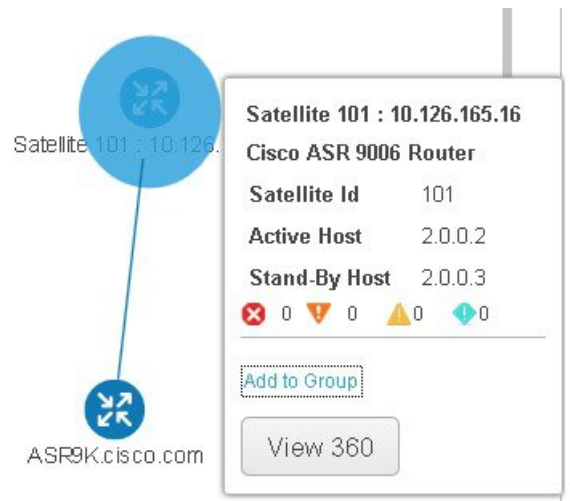
## View Cisco ASR 9000 Host-Satellite Topologies in the Topology Map

You can visualize the Cisco ASR 9000 host-satellite topologies and see, at a glance, whether there are active alarms on the host or satellites. From the topology map you can drill down to get further information about the host and satellite devices.

You can easily identify a satellite in the map by its label which includes the satellite ID and the IP address of the Cisco ASR 9000 host.



**Note** To see the links between the devices in the satellite topology, you must enable the Inter-Chassis Control and ICCP links in the Link Types filter (top right corner above the map). ICCP protocol is used for host to host links.



To view Cisco ASR 9000 host-satellite topologies in the map:

- Step 1** Choose **Maps > Network Topology** in the left navigation pane.
- Step 2** From the Groups pane on the left, select the group that contains the Cisco ASR 9000 host and satellites. The topology map displays all the devices in the selected group.
- Step 3** Locate the host or one of the satellites in the map.
- Step 4** To display the links between host and satellites:
  - Click the filter icon in the topology toolbar and choose **Link Types**.
  - Check the Control Plane, Inter\_Chassis\_Control, and ICCP check boxes, then click **OK**.
- Step 5** Click a satellite to launch a popup showing the satellite ID as well as the ID of the active and standby hosts.
- Step 6** Click View 360 in the popup to see more details about the satellite and its hosts in the Satellite 360 view, as described in [Identify the Satellites Connected to a Cisco ASR 9000 Host, on page 236](#).

## Identify the Satellites Connected to a Cisco ASR 9000 Host

The Device 360 view for a selected Cisco ASR 9000 host contains information about the device itself as well as about the satellites connected to the host.

To identify the satellites connected to a Cisco ASR 9000 host:

- Step 1** Choose **Inventory > Network Devices** in the left navigation pane.

**Step 2** From the Device Group pane on the left, select the group that contains the Cisco ASR 9000 host.

**Step 3** Locate the host in the device list on the right.

**Step 4** Click the “i” icon next to the device IP address/DNS to open the Device 360 view for the host.

**Note** You can also access the Device 360 view from the map by clicking on the device and then clicking **View 360** in the displayed popup.

The Satellites tab lists the satellites that are associated with the host and provides basic information about each satellite, such as type, description, IP address, and MAC address. It also indicates whether the satellite is currently connected to or disconnected from the host. The Satellites tab is only present in the Device 360 view for Cisco ASR 9000 host and satellite devices.

**Step 5** Click the “i” icon next to the IP address in the Satellites tab to open the Device 360 view for the satellite. The Hosts tab lists the active and standby hosts associated with that satellite.

**Device 360**

**ASR9K.cisco.com** ● ✓  
 10.126.165.16 Cisco ASR 9006 Router  
 BGL LAB  
 up for 20 days 2 hrs 33 mins 28 secs

OS Type IOS XR  
 OS Version 5.2.0[Default]  
 Last Config Change January 19, 2015 12:25:44 PM IST  
 Last Inventory Change

CPU Utilization (%) No Data Available  
 Memory Utilization (%) No Data Available

Modules Interfaces Neighbors Circuit/VC **Satellites**

Name	Type	Status	Descri...	IP Address	MAC
Satellite 101 : 1...	ASR90...	CONNE...		10.0.101.1 ⓘ	501c
Satellite 102 : 1...	ASR90...	CONNE...		10.0.102.1 ⓘ	501c
Satellite 103 : 1...		DISCOV...		10.0.103.1 ⓘ	

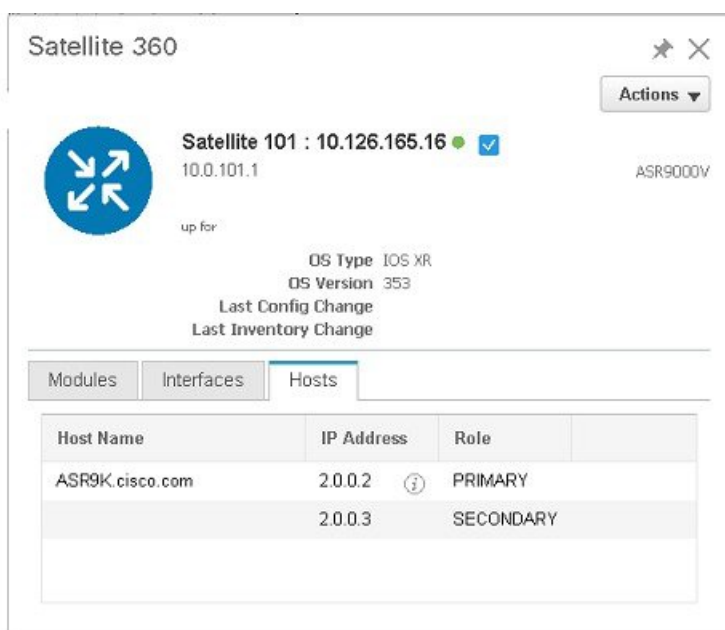
## Identify the Hosts Connected to a Satellite

Usually the links in the map will clearly show the satellite topology including the host and the connected satellites. If for some reason the satellites are shown without links, it is easy to identify the hosts with which a satellite is associated.

To identify the hosts connected to a satellite:

- 
- Step 1** Choose **Maps > Network Topology** in the left navigation pane.
- Step 2** From the Device Groups pane on the left, select the group that contains the Cisco ASR 9000 host and satellites. The map displays all the devices in the selected group.
- Step 3** Click a satellite device, identified by its label which begins with **Satellite ID**.
- Step 4** In the displayed popup, click **View 360** to launch the Satellite 360 view.

The Hosts tab in the Satellite 360 view lists the host devices to which the satellite is connected and their role, either active or standby.



## Monitor Cisco ASR 9000 nV Satellites for Faults

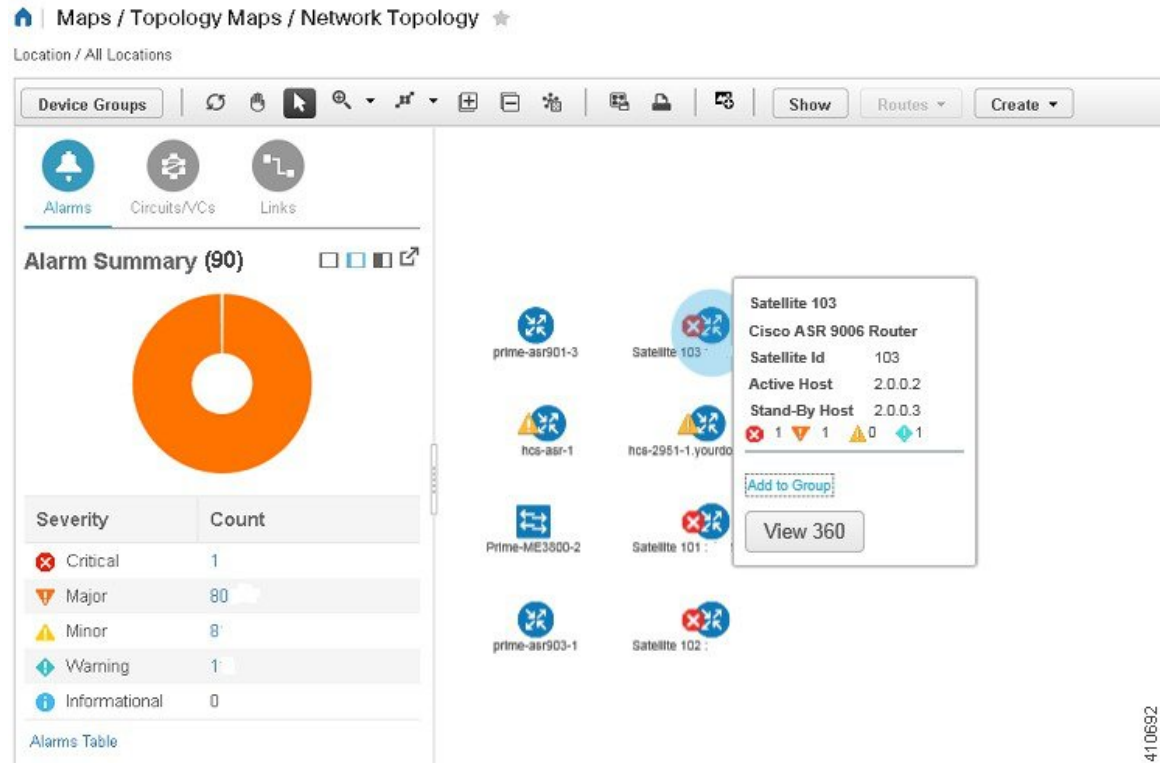
When a fault occurs on a satellite, Cisco EPN Manager associates (localizes) the fault to either the host device or satellite device depending on the fault type.

- If a fault occurs on a physical entity, such as a port, fan, or module, Cisco EPN Manager identifies the satellite device as the fault location.
- If the fault occurs on a logical entity such as a sub-interface, Cisco EPN Manager identifies the host device as the fault location because the sub-interface is configured on the host.

If an alarm occurs on dual-homed satellite, the alarm is duplicated, with one alarm on the active host and another on the standby host.

## View Satellite Faults in a Topology Map

In the topology map, you will see an alarm badge overlaid on the alarm source: the satellite device, the host device, or the link between the satellite and host device.




If there are several alarms on the same entity, the alarm badge severity represents that of the most severe alarm.

Right-click the alarmed entity to display a popup that shows the count of all active alarms related to the entity. Link-related alarms, such as Link Down, generate an alarm badge on the relevant link in the topology map.

## View Satellite Faults Using a Device 360 View

To find out which objects are affected by the device alarms, click View 360 from the popup menu and check the Affected Objects column. If you want to view details about a specific alarm, click the alarmID hyperlink.

Device 360



**ASR9001-165.7**

10.126.165.7

up for 21 days 1 hrs 40 mins 51 secs

OS Type

OS Version

Last Config Change May 11, 2015 1:49:53 AM EDT

Last Inventory Change May 12, 2015 4:28:31 AM EDT

View

Actions

Cisco ASR 9001 Router

CPU Utilization (%)

Memory Utilization (%)

6h

6h







Alarms

Modules

Interfaces

Neighbors

Circuit/VC

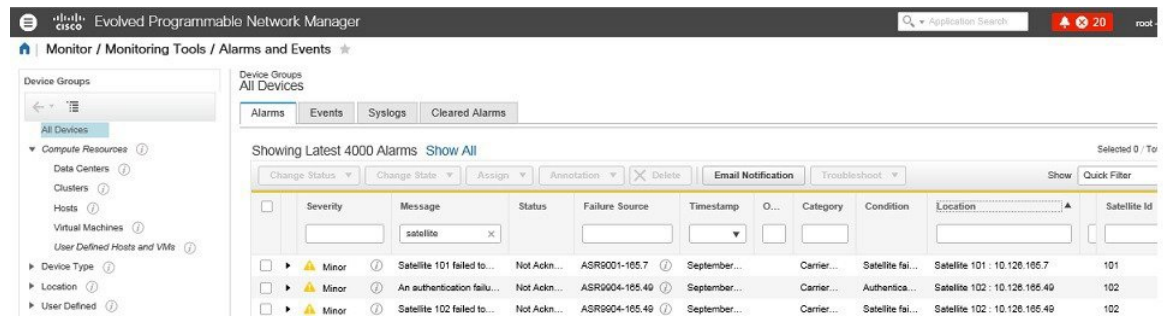
Severity	Condit...	Timpstamp	Affected Obj...	alarmID
	Authent...	May 12, 2015 4:...	Not Available	1029091
	No Lon...	May 12, 2015 4:...	GigabitEthe... 	1029124
	Link down	May 11, 2015 9:...	TenGigE0/0... 	1029093
	Satellit	May 11, 2015 9:...	Satellite 700...	1029092

403244

## View Satellite Faults in the Alarms and Events Table

To get satellite alarm information from the Alarm table, choose **Monitor > Monitoring Tools > Alarms and Events**, then click the **Alarms** tab.

Cisco EPN Manager lists the host device as the Failure Source. The Satellite ID and Location fields identify the satellite source.



406012

## Monitor a Cisco ASR 9000 nV Edge Cluster

- [Minimum Device and OS Requirements for nV Edge, on page 241](#)
- [View a nV Edge Cluster in the Topology Map, on page 241](#)
- [Identify the Primary and Backup Devices in a Cluster, on page 242](#)
- [Monitor and Troubleshoot a Cisco ASR 9000 nV Edge Cluster Service, on page 243](#)

nV Edge is a feature where two or more Cisco ASR 9000 Series Router chassis are combined to form a single logical switching or routing entity. This allows you to operate two Cisco ASR 9000 Series Router platforms as a single virtual Cisco ASR 9000 Series system. Effectively, they can logically link two physical chassis with a shared control plane, as if the chassis were two route switch processors (RSPs) within a single chassis.

There are two types of links in the nV edge topology:

- Control links, used for control traffic.
- Inter-Rack links, used for data generation and forwarding of data between chassis.

## Minimum Device and OS Requirements for nV Edge

The following are the minimum device and device operating system requirements for nV edge:

- 2 Cisco ASR 9000 devices running Cisco IOS XR 5.2.0
- 4 10G SFP (for IRL)
- 4 1G SFP (for cluster/control links)
- 2 RSP nodes per chassis, with the exception of the Cisco ASR 9001 which is a single RSP system that supports cluster configuration

Additional support may be available. See the [Cisco Evolved Programmable Network Manager Supported Devices](#).

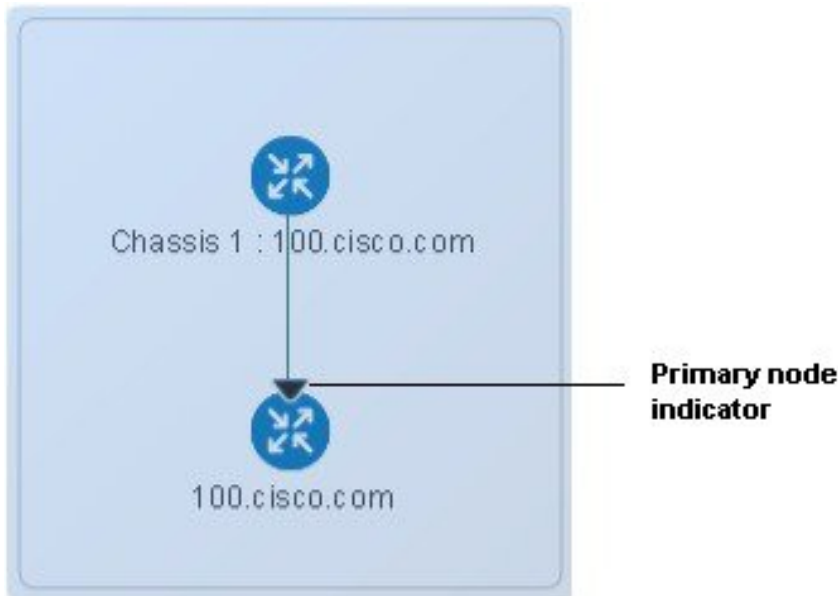
## View a nV Edge Cluster in the Topology Map

The nV edge cluster is represented in the topology map as a single object consisting of two linked chassis, one primary and one backup.

To view the Cisco ASR 9000 nV Edge topology in the map:

- Step 1** Choose **Maps > Network Topology** in the left navigation pane.

- Step 2** From the Groups pane on the left, select the group that contains the Cisco ASR 9000 cluster. The topology map displays all the devices in the selected group.
- Step 3** Click the primary or backup chassis. Note that both chassis are selected and a popup opens representing the two chassis together. You cannot access each chassis individually.
- Step 4** To display links in the cluster topology:
- Click the filter icon in the topology toolbar, then choose **Link Types**.
  - Check the Control Plane and Inter\_Chassis\_Control check boxes, then click **OK**.



## Identify the Primary and Backup Devices in a Cluster

The topology map clearly shows which chassis is primary and which is the backup chassis. Further details about the chassis are provided in the Device 360 view.

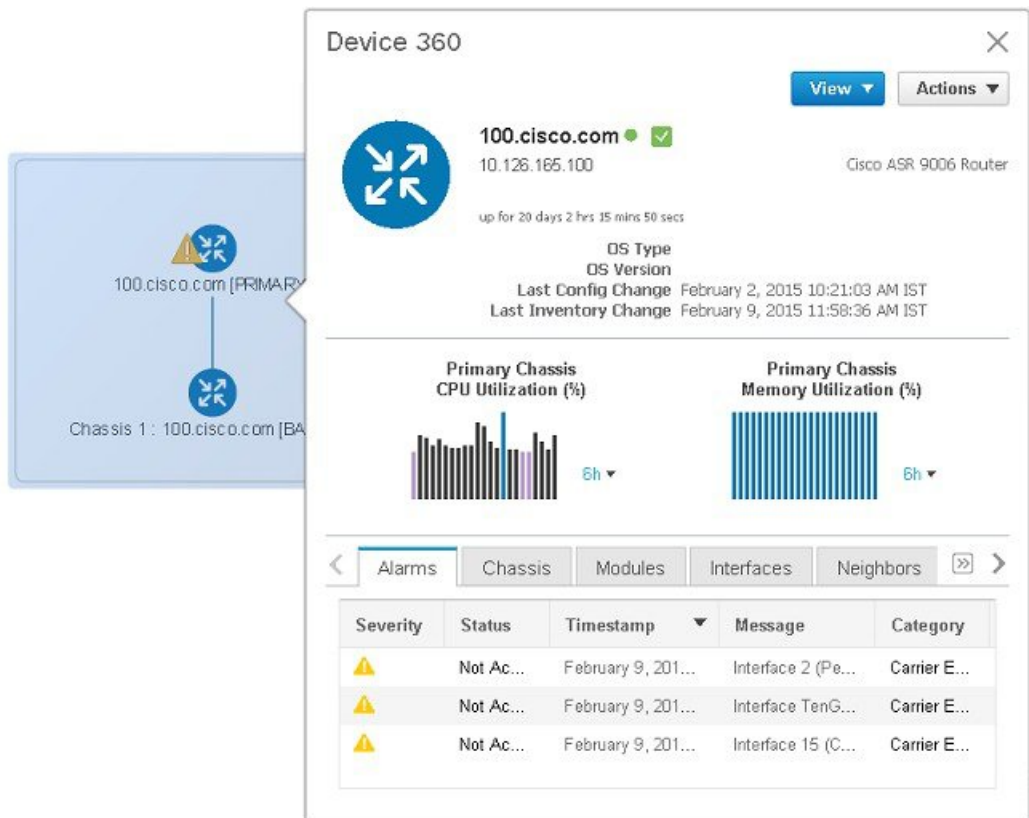
To identify the primary and backup devices and get more information:

- Step 1** Choose **Maps > Network Topology** in the left navigation pane.
- Step 2** From the Device Groups pane on the left, select the group that contains the Cisco ASR 9000 cluster setup. The map displays all the devices in the selected group.
- Step 3** Click the cluster representation.
- Step 4** In the displayed popup, click **View 360**.
- Note that the Chassis tab in the Device 360 view lists and identifies the chassis in the cluster and provides information as to their status and their role (primary or backup).



## Monitor and Troubleshoot a Cisco ASR 9000 nV Edge Cluster Service

Cisco EPN Manager displays alarm indicators on the cluster and provides graphs showing CPU and memory utilization for the primary chassis in the Device 360 view.







## CHAPTER 11

# Manage Reports

- [Reports Overview, on page 245](#)
- [Available Reports, on page 245](#)
- [Create, Schedule, and Run a New Report, on page 261](#)
- [Customize Report Results, on page 262](#)
- [Report Output Examples: Web GUI Output and CSV File Output, on page 262](#)
- [Troubleshooting Tips for an Empty Report, on page 264](#)

## Reports Overview

Cisco EPN Manager reports provide information about system and network health as well as fault information. You can customize and schedule reports to run on a regular basis. Reports can present data in a tabular, or graphical format (or a mixture of these formats). You can also save reports in CSV or PDF format. The CSV or PDF files can be saved on the Cisco EPN Manager server for later download, or sent to an e-mail address.

Cisco EPN Manager provide the following type of data:

- **Current**—Provides a snapshot of data that is not time-dependent.
- **Historical**—Periodically retrieves data from the device and stores it in the Cisco EPN Manager r database.
- **Trend**—Generates a report using aggregated data, which is collected and summarized as minimums, maximums, and averages.

With Cisco EPN Manager , you can filter these reports based on a specific criteria. For example, IPSLA Y.1731 reports can be filtered based on probes and PWE3 reports can be filtered based on Virtual Connection Identifier (VCID). You can also export reports, sort reports into logical groups, and archive reports for long-term storage.

## Available Reports

The Reports Launch Pad provides access to the following Cisco EPN Manager reports:

- [Carrier Ethernet Performance Reports, on page 246](#)
- [Optical Performance Reports, on page 253](#)
- [Performance Reports, on page 258](#)
- [Network Summary Reports, on page 258](#)
- [Device Reports, on page 259](#)

## Carrier Ethernet Performance Reports

This section lists the Carrier Ethernet (CE) Performance reports supported by Cisco EPN Manager . It also includes the monitoring policies that must be enabled so that the proper report data is collected. For more information about monitoring policies, see [How Device Health and Performance Is Monitored: Monitoring Policies, on page 193](#).

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
IPSLA Graphs	Graphical representation of average delay backward, average delay forward, average delay two-way, jitter forward, jitter backward, average backward packet loss ratio, average forward packet loss ratio, and availability.	<i>IPSLA</i>  For details about the IPSLA monitoring policy, see <a href="#">IP SLA Monitoring Policy, on page 770</a> .	Response Time Avg, Response Time Max, Response Time Min, Jitter Neg DS Avg, Jitter Neg SD Avg, Jitter Pos DS Avg, Jitter Pos SD Avg, Packet Loss Overall Util Avg, Packet Loss DS Util Avg, Packet Loss SD Util Avg, Latency One Way SD Avg, Latency One Way SD Max, Latency One Way SD Min, Latency One Way DS Avg, Latency One Way DS Max, Latency One Way DS Min
IPSLA Statistics	Tabular representation of probe index, IPSLA probe type, TOS, target IP, VRF name, average delay two-way, average delay forward, average delay backward, packet loss ratio forward, packet loss ratio backward, average jitter forward, average jitter backward, average backward packet loss ratio, average forward packet loss ratio, and availability.	<i>IPSLA</i>  For details about the IPSLA monitoring policy, see <a href="#">IP SLA Monitoring Policy, on page 770</a> .	Jitter Neg DS Avg, Jitter Neg SD Avg, Jitter Pos DS Avg, Jitter Pos SD Avg, Packet Loss Overall Util Avg, Packet Loss DS Util Avg, Packet Loss SD Util Avg, Latency One Way SD Avg, Latency One Way SD Max, Latency One Way SD Min, Latency One Way DS Avg, Latency One Way DS Max, Latency One Way DS Min

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
IPSLA Top N	Tabular representation of probe index, IPSLA probe type, TOS, target IP, VRF name, average delay two-way, maximum delay two-way, minimum delay two-way, average delay forward, maximum delay forward, minimum delay forward, average delay backward, maximum delay backward, minimum delay backward, average forward packet loss ratio, average backward packet loss ratio, jitter forward, jitter backward and availability.	<i>IPSLA</i> For details about the IPSLA monitoring policy, see <a href="#">IP SLA Monitoring Policy</a> , on page 770.	Response Time Avg, Response Time Max, Response Time Min, Jitter Neg DS Avg, Jitter Neg SD Avg, Jitter Pos DS Avg, Jitter Pos SD Avg, Packet Loss Overall Util Avg, Packet Loss DS Util Avg, Packet Loss SD Util Avg, Latency One Way SD Avg, Latency One Way SD Max, Latency One Way SD Min, Latency One Way DS Avg, Latency One Way DS Max, Latency One Way DS Min
IPSLA Y.1731 Graphs	Graphical representation of average delay backward, average delay forward, jitter two-way, jitter forward, jitter backward, average backward frame-loss ratio, average forward frame-loss ratio, and availability of the Y.1731 probe.	<i>IPSLA Y.1731</i> For details about the IPSLA Y.1731 monitoring policy, see <a href="#">IP SLA Y.1731 Monitoring Policy</a> , on page 768.	Average Delay Two Way, Average Delay Forward, Average Delay Backward, Average Positive Jitter Forward, Average Negative Jitter Forward, Average Positive Jitter Backward, Average Negative Jitter Backward, Average Forward Frame Loss Ratio, Average Backward Frame Loss Ratio
IPSLA Y.1731 Statistics	Tabular representation of operation type, CFM domain, source, destination, frame type, average delay two-way, average delay forward, average delay backward, average jitter, forward frame loss ratio, backward frame loss ratio, average forward jitter, average backward jitter, and availability of the Y.1731 probe.	<i>IPSLA Y.1731</i> For details about the IPSLA Y.1731 monitoring policy, see <a href="#">IP SLA Y.1731 Monitoring Policy</a> , on page 768.	Average Delay Two Way, Average Delay Forward, Average Delay Backward, Average Forward Frame Loss Ratio, Average Backward Frame Loss Ratio, Average Jitter

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
IPSLA Y.1731 Top N	Tabular representation of operation type, CFM domain, source, destination, frame type, average delay two-way, maximum delay two-way, minimum delay two-way, average delay forward, maximum delay forward, minimum delay forward, average delay backward, maximum delay backward, minimum delay backward, average forward frame loss ratio, maximum forward frame loss ratio, minimum forward frame loss ratio, average backward frame loss ratio, maximum backward frame loss ratio, minimum backward frame loss ratio, jitter forward, jitter backward, and availability of the devices that are configured using the Y.1731 technology.	<i>IPSLA Y.1731</i> For details about the IPSLA Y.1731 monitoring policy, see <a href="#">IP SLA Y.1731 Monitoring Policy</a> , on page 768.	Average Delay Two Way, Average Delay Forward, Average Delay Backward, Average Positive Jitter Forward, Average Negative Jitter Forward, Average Positive Jitter Backward, Average Negative Jitter Backward, Average Forward Frame Loss Ratio, Average Backward Frame Loss Ratio
Interface Graphs	Graphical representation of the interface traffic statistics over time: in traffic, out traffic, in utilization and out utilization.	<i>Interface Health</i> For details about the Interface Health monitoring policy, see <a href="#">Interface Health Monitoring Policy</a> , on page 768.	Statistics

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Interface Top N	Tabular representation of Top N reports of interface traffic statistics: maximum in traffic, average in traffic, maximum out traffic, average out traffic, maximum in utilization, maximum out utilization and current in utilization, current out utilization, in errors, out errors, in discards, out discards and interface availability.	<i>Interface Health</i>  For details about the Interface Health monitoring policy, see <a href="#">Interface Health Monitoring Policy, on page 768</a> .	Statistics
Interface Traffic	Tabular representation of interface traffic statistics: in traffic rate, out traffic rate, in utilization, out utilization, in errors, out errors, in discards, out discards, CRC errors and percentage.	<i>Interface Health</i>  For details about the Interface Health monitoring policy, see <a href="#">Interface Health Monitoring Policy, on page 768</a> .	Statistics and CRC
Link Utilization	<p>Tabular representation of A end device, A end interface, A member of, A end in utilization, A end out utilization, Z end device, Z end interface, Z member of, event time, and the interface utilization of the interfaces participating in the link, including the link aggregate group they belong to.</p> <p><b>Note</b> The prerequisite for this report is to have CDP/LLDP enabled links in the network.</p>	<i>Interface Health</i>  For details about the Interface Health monitoring policy, see <a href="#">Interface Health Monitoring Policy, on page 768</a> .	Statistics

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Optical SFP interface report	Tabular representation of transmit/receive power levels of the devices for interfaces. Includes device name, interface name, RxPower, TxPower, EVENTTIME.	<i>Optical SFP</i>  For more details about the Optical SFP monitoring policy, see <a href="#">Optical SFP Monitoring Policy</a> , on page 771.	Optical Tx Power, Optical Rx Power
PWE3 Statistics	Tabular representation of PWE3 traffic and availability statistics including device name, IP address, VC ID, peer address, VC type, current in bit rate, current out bit rate, current in byte rate, current out byte rate, current in packet rate, current out packet rate, global availability, in availability and out availability.	<i>Pseudowire Emulation Edge to Edge</i>  For details about the Pseudowire Emulation Edge to Edge monitoring policy, see <a href="#">Pseudowire Emulation Edge to Edge Monitoring Policy</a> , on page 769.	PW VC Perf Total In HC Packets Rate, PW VC Perf Total In HC Bytes Rate, PW VC Perf Total Out HC Packets Rate, PW VC Perf Total Out HC Bytes Rate, PW VC Oper Status Up, PW VC Inbound Oper Status Up, PW VC Outbound Oper Status Up, PW VC Oper Status Down, PW VC Perf Total In HC Packets, PW VC Perf Total In HC Bytes, PW VC Perf Total Out HC Packets, PW VC Perf Total Out HC Bytes, PW VC Inbound Oper Status Down, PW VC Outbound Oper Status Down
PWE3 Top N	Tabular representation of Top N reports of PWE3 statistics including device name, IP address, VC ID, peer address, VC type, average in byte rate, average out byte rate, maximum in byte rate, maximum out byte rate, average in bit rate, average out bit rate, maximum in bit rate, maximum out bit rate, average in packet rate, average out packet rate, maximum in packet rate, maximum out packet rate, global inbound availability and global outbound availability.	<i>Pseudowire Emulation Edge to Edge</i>  For details about the Pseudowire Emulation Edge to Edge monitoring policy, see <a href="#">Pseudowire Emulation Edge to Edge Monitoring Policy</a> , on page 769.	PW VC Perf Total In HC Packets Rate, PW VC Perf Total In HC Bytes Rate, PW VC Perf Total Out HC Packets Rate, PW VC Perf Total Out HC Bytes Rate, PW VC Oper Status Up, PW VC Inbound Oper Status Up, PW VC Outbound Oper Status Up, PW VC Oper Status Down, PW VC Perf Total In HC Packets, PW VC Perf Total In HC Bytes, PW VC Perf Total Out HC Packets, PW VC Perf Total Out HC Bytes, PW VC Inbound Oper Status Down, PW VC Outbound Oper Status Down



Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
PWE3 Traffic Graphs	Graphical representation of PWE3 traffic including average in bit rate, average out bit rate, average in byte rate, average out byte rate, average in packet rate, average out packet rate, global availability, in availability and out availability.	<i>Pseudowire Emulation Edge to Edge</i>  For details about the Pseudowire Emulation Edge to Edge monitoring policy, see <a href="#">Pseudowire Emulation Edge to Edge Monitoring Policy</a> , on page 769.	PW VC Perf Total In HC Packets Rate, PW VC Perf Total In HC Bytes Rate, PW VC Perf Total Out HC Packets Rate, PW VC Perf Total Out HC Bytes Rate, PW VC Oper Status Up, PW VC Inbound Oper Status Up, PW VC Outbound Oper Status Up, PW VC Oper Status Down, PW VC Perf Total In HC Packets, PW VC Perf Total In HC Bytes, PW VC Perf Total Out HC Packets, PW VC Perf Total Out HC Bytes, PW VC Inbound Oper Status Down, PW VC Outbound Oper Status Down
Link Optical SFP Power Level Reports	Tabular representation of the A end device, A end interface, Z end device, Z end interface, and their Tx and Rx power levels.  <b>Note</b> The prerequisite for this report is to have CDP/LLDP enabled links in the network.	<i>Optical SFP</i>  For more details about the Optical SFP monitoring policy, see <a href="#">Optical SFP Monitoring Policy</a> , on page 771.	Optical Tx Power, Optical Rx Power

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
QoS Policing	Tabular representation of the details about the policy map: ClassMap. The details include, direction of the policy map, average exceed byte rate, maximum exceed byte rate, maximum exceed date, average violate byte rate, maximum violate byte rate, maximum violate date, average conformed byte rate, maximum conformed byte rate, maximum conformed date, CIR current rate and PIR current rate. Also, graphical representation of exceed, violate and conformed byte rates.	<i>Quality of Service</i> For details about the Quality of Service monitoring policy, see <a href="#">Quality of Service Monitoring Policy</a> , on page 769.	Conformed Bytes Rate, Exceeded Bytes Rate, Violated Bytes Rate, Exceeded Packets, Violated Bytes, CIR, Conformed Bytes, Exceeded Bytes, PIR

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
QoS Policy	Graphical and tabular representation of the details about the policy map: ClassMap. The details include, direction of the policy map, average pre-policy byte rates, maximum pre-policy byte rates, average post-policy byte rates, maximum post-policy byte rates, maximum pre-policy dates, maximum post-policy dates, average drop in percentage, maximum drop in percentage, maximum drop date, average pre-policy of CIR, average interface speed in percentage, maximum pre-policy of CIR, maximum interface speed in percentage, average pre-policy of CIR, maximum pre-policy of CIR and interface speed date. Also, graphical representation of pre-policy, post-policy, drop bit rate, and drop percentage.	<i>Quality of Service</i> For details about the Quality of Service monitoring policy, see <a href="#">Quality of Service Monitoring Policy</a> , on page 769.	Drop Bytes Rate, Drop Percent, Post-Policy Bytes Rate, Pre-Policy Bytes Rate, Pre-Policy Percent of CIR, Post-Policy Percent of CIR, CIR, Post-Policy Rate (Bytes/Sec), Pre-Policy Bytes

## Optical Performance Reports

[Table 10: Optical Performance Reports](#) lists the Optical Performance reports supported by Cisco EPN Manager. For all the graphical reports, ensure that you select a maximum of four interfaces when you schedule or run these reports. For all the tabular reports, use the Show field to specify the number of records to be displayed in a page when you schedule or run these reports.

The performance data displayed when you generate these reports depend on the monitoring policy parameter that you activate when you enable the monitoring policy. For a detailed list of monitoring type and the associated performance counters, see [Monitoring Policies Reference](#), on page 767. For more information about monitoring policies, see [Monitor Device and Network Health and Performance](#), on page 193. For information about how to interpret the report results, see [Report Output Examples: Web GUI Output and CSV File Output](#), on page 262.



**Note** Enable the *Optical 1 day* or *Optical 15 mins* monitoring policies to populate data for these reports.

**Table 10: Optical Performance Reports**

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
Ethernet	Ethernet Reports—NCS1K, NCS2K and NCS4K	<p>Graphical and tabular reports that lists the total number of packets requested by the higher-level protocols to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. The details also include total number of multicast frames transmitted error free, total number of packets requested by higher-level protocols, total number of transmitted octets, total number of octets received on the interface and number of received packets that were discarded because of errors.</p> <p>To customize the report output for a new report, choose <b>Reports &gt; Report Launch Pad &gt; Ethernet</b>, click <b>New</b>, and then click <b>Customize</b> in the <b>Settings</b> area .</p> <p>To customize the report output for an existing report, choose <b>Reports &gt; Report Launch Pad &gt; Ethernet</b>, click the required report link, and then click <b>Customize</b> in the <b>Settings</b> area.</p>	<p><i>Optical 1 day</i> or <i>Optical 15 mins</i></p> <p>For details about the information collected by optical monitoring policies, see <a href="#">Monitoring Policies Reference, on page 767</a>.</p> <p>For information about how to interpret the report results, see <a href="#">Report Output Examples: Web GUI Output and CSV File Output, on page 262</a>.</p>	Ethernet

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
OTN	Section Monitoring NEnd & FEnd Reports- NCS1K, NCS2K and NCS4K	Graphical and tabular reports that list the OTN section monitoring details of devices and interfaces in the OTN circuit type. The details include number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, and number of failure counts.	<i>Optical 1 day</i> or <i>Optical 15 mins</i> For details about the information collected by optical monitoring policies, see <a href="#">Monitoring Policies Reference, on page 767</a> . For information about how to interpret the report results, see <a href="#">Report Output Examples: Web GUI Output and CSV File Output, on page 262</a> .	OTN DWDM Infrastructure <sup>1</sup>
	Path Monitoring NEnd & FEnd Reports	Graphical and tabular reports that list the OTN path monitoring details of devices and interfaces in OTN circuit type. They provide details such as number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, and number of failure counts.		
	Forward Error Correction Reports- NCS1K, NCS2K and NCS4K	Graphical and tabular reports that list the OTN forward error correction details of devices and interfaces in the OTN circuit type. The details include the number of bit errors corrected, number of uncorrectable words, and Pre-forward error correction based bit error counts detected during the performance monitoring time interval.		
	Tandem Connection Monitoring NEnd & FEnd Reports	Graphical and tabular reports that provide the tandem connection monitoring details for the devices and interfaces in the OTN circuit type. The details include number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, and number of failure counts.		OTN
	GFP Statistics Reports–NCS2K and NCS4K	Graphical and tabular reports that provide the generic framing procedure (GFP) statistics for the devices in the OTN circuit type. The GFP statistics include number of GFP frames and bytes received and transmitted, number of single and multiple bit errors received, number of packets received with CRC errors, invalid GFP type, and invalid CID, number of CMF frames received and transmitted, and number of cHEC and tHEC multiple bit errors.		OTN DWDM Infrastructure <sup>1</sup>

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
Physical	Optical Power Reports-NCS1K, NCS2K, and NCS4K	Graphical and tabular reports that provide the average, minimum, and maximum percentage of optical input and output power of the received and transmitted signal for devices in a physical circuit type.	<i>Optical 1 day</i> or <i>Optical 15 mins</i> For details about the information collected by optical monitoring policies, see <a href="#">Monitoring Policies Reference, on page 767</a> .  For information about how to interpret the report results, see <a href="#">Report Output Examples: Web GUI Output and CSV File Output, on page 262</a> .	Physical DWDM Infrastructure <sup>1</sup>
	Laser Bias Current Reports-NCS1K, NCS2K, and NCS4K	Graphical and tabular reports that provide the average, minimum, and maximum percentage of laser bias current. The laser bias current is the normalized value expressed as the integer percentage.		
	Optical Physical Report -NCS1K, NCS2K, NCS4K	Graphical and tabular reports that provide the average, minimum, and maximum value of optical power on the unidirectional port. The details include the average, minimum and maximum Optical Service Channel power level The details of average, minimum and maximum optical signal-to-noise ratio, optical power warning, chromatic dispersion, second order polarization mode dispersion, polarization dependent loss, differential group delay, polarization change rate, and phase noise.		

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
SDH Or SONET	SDH Regenerator Section Report	Graphical and tabular reports that provide the performance monitoring details of the SDH regenerator section layer for the devices in your network. The details include the number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, number of errored block, and number of out-of-frame seconds.	<i>Optical 1 day</i> or <i>Optical 15 mins</i> For details about the information collected by optical monitoring policies, see <a href="#">Monitoring Policies Reference, on page 767</a> .  For information about how to interpret the report results, see <a href="#">Report Output Examples: Web GUI Output and CSV File Output, on page 262</a> .	SDH/SONET  DWDM Infrastructure <sup>1</sup>
	SDH Multiplex Section NEnd & FEnd Reports - NCS2K	Graphical and tabular reports that provide the performance monitoring details of SDH multiplex section layer for the devices in your network. The details include number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, number of errored blocks, number of failure counts, protection switching — Switching count, ring count, span count, working count, duration, ring duration, span duration and working duration.		
	SDH Multiplex Section NEnd & FEnd Reports - NCS4K	Graphical and tabular reports that provide the performance monitoring details of SDH multiplex section layer for the devices in your network. The details include number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, and number of errored blocks.		
	SONET Section Report	Graphical and tabular reports that provide performance monitoring details of SONET section layer for the devices in your network. The details include number of coding violations, number of errored seconds, number of severely errored seconds, and number severely errored frame seconds.		
	SONET Line NEnd & FEnd Reports - NCS2K	Graphical and tabular reports that provide performance monitoring details of SONET line layer for the devices in your network. The details include number of coding violations, number of errored seconds, number of severely errored seconds, number of unavailable seconds, number of failure counts, protection switching— Switching count, ring count, span count, working count, duration, ring duration, span duration and working duration.		
	SONET Line NEnd & FEnd Reports - NCS4K			

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
		Graphical and tabular reports that provide performance monitoring details of SONET line layer for the devices in your network. The details include number of coding violations, number of errored seconds, number of severely errored seconds, number of unavailable seconds, and number of failure counts.		

1. You must activate this parameter for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices.

## Performance Reports

This section lists the basic performance reports supported by Cisco EPN Manager . It also lists the monitoring policies and parameters that must be enabled for each of the report type. These reports are applicable for both Optical and Carrier Ethernet technologies.



### Note

These reports are not supported for Cisco NCS 2000 devices.

For more information about monitoring policies, see [Monitor Device and Network Health and Performance, on page 193](#).

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Environmental Temperature	Tabular representation of current, average, minimum, and maximum temperature for network devices.	<i>Device Health</i> For details about the Device Health monitoring policy, see <a href="#">Device Health Monitoring Policy, on page 767</a> .	Environment Temperature
Threshold Violations	Lists the threshold violation alarms data (source, event type, category and description) for your network in a table.	<i>Interface Health</i> For details about the Device Health monitoring policy, see <a href="#">Device Health Monitoring Policy, on page 767</a> .	Admin Status Up/Down Operational Status Up/Down Admin Status Up and Operational Status Down Percentage

## Network Summary Reports

This section lists the Network Summary reports supported by Cisco EPN Manager . These reports provide information about the health of the network.



Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Polled
Link Flap Report	Tabular representation of the A end device, A end interface, Z end device, Z end interface, link name and the number of flaps.	NA	NA

## Device Reports

This section lists the device reports supported by Cisco EPN Manager . It also lists the monitoring policies and parameters that must be enabled for each of the report type. These reports are applicable for both Optical and Carrier Ethernet technologies.



**Note** Device reports are not supported for Cisco NCS 2000 devices.

For more information about monitoring policies, see [Monitor Device and Network Health and Performance, on page 193](#).

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Alarm Report	List of alarms for devices in the network. Includes severity, message, status, failure source, time stamp, creation time, device timestamp, owner, category, condition, location, service affecting, satellite ID.	NA	NA
CPU Utilization	Table listing all devices with their average CPU usage for a specified time period.	<i>Device Health</i> For details about the Device Health monitoring policy, see <a href="#">Device Health Monitoring Policy, on page 767</a> .	CPU Utilization
Detailed Hardware	Table listing all devices in ascending order according to their average CPU usage for a specified time period.	NA	NA
Detailed Software	Hardware information for the entire inventory or device types (for example, Switches and Hubs, Routers, and Optical Transport). Provides system information and the last time the system was updated.	NA	NA
Device Availability	Table listing all the available devices in the network and their reachability percentage.	NA	NA
Device Credential Verification	The credential status of the devices in your network. Includes the login, reachability, and protocol statuses of each device. Also, includes the last modified date and time for the device.	NA	NA

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Event Report	List of events for devices in your network. Includes description, failure source, time stamp, device timestamp, severity, category, condition.	NA	NA
Interface Detail	Interface details for the devices in your network. Includes device name, port name, port description, MAC address, admin status, operational status.	NA	NA
Inventory	Basic inventory data for the devices in your network. Includes count of controllers by model, count of controllers by software version, controller inventory, count of APs by model, count of APs by software version, AP inventory, disassociated AP(s), autonomous AP inventory, maintenance mode AP(s), count of MSEs by version, MSEs, count of switches by model, count of switches by version, switch inventory, switch devices software images, count of routers by model, count of routers by version, router inventory, router devices software images, count of Cisco Interfaces and Modules devices by model, count of Cisco Interfaces and Modules devices by software version, Cisco Interfaces and Modules devices inventory, Cisco Interfaces and Modules - software images, count of storage networking devices by model, count of storage networking devices by software version, storage networking devices inventory, storage networking devices - software images, count of security and VPN by model, count of security and VPN by software version, security and VPN inventory.	NA	NA
Wired Detailed Device Inventory	<p>Detailed inventory data for the wired devices in your network. Includes system information, chassis information, module information, module port interfaces, VLAN interfaces, software image information, memory pool information, flash devices, flash partition, flash file.</p> <p><b>Note</b> Up to 5 devices can be selected if you want to run the report immediately without saving it. To include more than 5 devices, save or schedule the report.</p>	NA	NA
Wired Device Availability	List of wired devices with highest availability in your network. Includes device name, average availability (%).	NA	NA
Wired Module Detail	Table listing detailed module information for wired devices in the network including device name, device IP, equipment name, number of ports, operational status, vendor equipment type, manufacturer, serial number, and UDI.	NA	NA

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Wired Port Attribute	Port attribute information such as admin status, operational status, mac address, etc. Includes VLAN ID, access mode VLAN, device IP address, description, MAC address, Admin status, operational status, type, MTU, speed, duplex, IsTrunk, trunk encapsulation	NA	NA
Device Health	CPU utilization, memory utilization, and availability information of the network devices for a specified time period. Includes minimum, maximum, and average for all CPU modules and memory pools on a device.	<i>Device Health</i> For details about the Device Health monitoring policy, see <a href="#">Device Health Monitoring Policy, on page 767</a> .	CPU Utilization
Memory Utilization	Memory utilization information for a specified time period. Includes information for all memory pools/modules.		Memory Pool Utilization

## Create, Schedule, and Run a New Report

The Report Launch Pad provides access to all Cisco EPN Manager reports from a single page. From this page, you can perform all report operations: Create, save, view, schedule, and customize.

To see more report details, hover the cursor over the tootip next to the report type.

To create, schedule, and run a new report:

- 
- Step 1** From the left sidebar, choose **Reports > Report Launch Pad**.
- Step 2** Locate the report you want to launch, then click **New**.
- Step 3** In the Report Details page, complete the required fields. You can filter the reports using Report by drop-down list, filter options vary according to the report type. The parameters shown in the Report Details page depend on the report type you chose. With some reports, you are required to customize the report results. For more information about how to customize a report result, see [Customize Report Results, on page 262](#).
- Step 4** If you plan to run this report later or as a recurring report, enter the required Schedule parameters.
- Step 5** To run the report, choose one of the following options:
- **Run**—Runs the report without saving the report setup.
  - **Save**—Saves this report setup without immediately running the report. If you have entered Schedule parameters, the report runs automatically at the scheduled date and time.
  - **Run and Save**—Saves this report setup and runs the report immediately.
  - **Save and Export**—Saves the report, runs it, and exports the results to a file. You will be prompted to:
    - Select the exported report's file format (CSV or PDF).
    - Choose whether to send an email when the report has been generated. If you choose this option, you must enter the destination email address and the email subject line content, and choose whether you want the exported file included as an attachment to the email.

When you are finished, click **OK**.

- **Save and Email**—Saves the report, runs it, exports the results as a file, and emails the file. You will be prompted to:

- Select the exported report file format.
- Enter the destination email address and the email subject line content.

When you are finished, click **OK**.

- **Cancel**—Returns to the previous page without running or saving this report.

## Customize Report Results

Many reports allow you to customize their results, letting you include or exclude different types of information. Reports that support this feature display a **Customize** button. Click this button to access the **Create Custom Report** page and customize the report results.

To customize a report result:

- Step 1** Choose the report you want to customize:
- Create a new report. Click **Reports > Report Launch Pad**.
  - Customize a recurring report. Click **Reports > Saved Report Templates** and, then click the report name hyperlink.
- Step 2** In the Report Details page, click **Customize**.
- Step 3** On the Create Custom Report page, complete the required information, then click **Apply** to confirm the changes.
- Step 4** Click **Save** in the Report Details page.

## Report Output Examples: Web GUI Output and CSV File Output

In this example, a section monitoring report is generated for Cisco NCS 2000 series devices that are available in the near end of the network. You can choose to view the result, either at the bottom of the Report Details page, or export the results to a CSV or PDF file. For more information about how to create and run a report, see [Create, Schedule, and Run a New Report, on page 261](#).

The following figure shows how the results are displayed at the bottom of the Report Details page.

SectionMonitoringNearEndNCS2K

Generated: 2015-Apr-02, 17:52:03 IST

Report By: Interfaces By Device

Devices: M6-235-140;rm1gte-m6-159;M6-235-139

Report Interval: 15 minutes

Reporting Period: Last 6 hours

Show: All records

Section Monitoring NEnd Report

Device Name	Device IP Address	Interface	DateTime	BBE-SM	BBER-SM	ES-SM	ESR-SM	SES-SM	SESR-SM	UAS-SM	FC-SM
M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:00:00 IST	0	0.00000	0	0.00000	0	0.00000	0	0
M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:15:00 IST	0	0.00000	0	0.00000	0	0.00000	0	0
M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:30:00 IST	0	0.00000	0	0.00000	0	0.00000	0	0
M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 13:00:00 IST	0	0.00000	0	0.00000	0	0.00000	0	0

403223

If you choose to export the result to a CSV file, the report is saved in the repository named `/localdisk/ftp/reports`. You can adjust the location of the report repository. For more information, see [Report Purging, on page 665](#).

The file naming convention for the CSV file is *ReportTitle\_yyyymmdd\_hhmmss.csv*, where *yyymmdd* is the year, month, and date, and *hhmmss* is the hours, minutes, and seconds when the report result was exported.

The following figure shows how the results are displayed in a CSV file.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Section Monitoring Report for Cisco NCS 2000 Series Devices											
2	Generated: 2015-04-02 17:52:03 IST											
3	Report By: Interfaces By Device											
4	Devices: M6-235-140;nmtgte-m6-159;M6-235-139											
5	Report Interval: 15 minutes											
6	Reporting Period: Last 6 hours											
7	Show: All records											
8												
9	Section Monitoring NEnd Report											
10	Device Name	Device IP Address	Interface	DateTime	BBE-SM	BBER-SM	ES-SM	ESR-SM	SES-SM	SESR-SM	UAS-SM	FC-SM
11	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:00:00 IST	0	0	0	0	0	0	0	0
12	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:15:00 IST	0	0	0	0	0	0	0	0
13	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:30:00 IST	0	0	0	0	0	0	0	0
14	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 13:00:00 IST	0	0	0	0	0	0	0	0

403224

The following table explains how you can interpret the section monitoring report result.

Column Name	Description
Device Name	Name of the device that is in the near end of the network.
Device IP Address	IP address of the device.
Interface	Interface name of the device.
DateTime	Date and time when the section monitoring data was collected for the device. The value in this column depends on the report interval that you chose when you created the report. The report interval can be 15 minutes or 24 hours.
BBE-SM	Number of background block errors for the device.
BBER-SM	Background block error ratio for the device.
ES-SM	Number of errored seconds for the device.
ESR-SM	Errored seconds ratio for the device.
SES-SM	Number of severely errored seconds for the device.
SESR-SM	Severely errored seconds ratio for the device.
UAS-SM	Number of unavailable seconds for the device.
FC-SM	Number of failure counts (AIS/RFI detected) for the device.

For detailed descriptions of performance counters that are displayed in the results of other optical performance reports, see [Performance Counters for Optical Monitoring Policies](#), on page 773 .

# Troubleshooting Tips for an Empty Report

If the report was run successfully but you do not have an output file that can be exported, you can try one of the following troubleshooting tips:

Check if you have...	For example:
...enabled the correct monitoring policy. For details on what monitoring policies must be enabled, see <a href="#">Monitoring Policies Reference, on page 767</a> .	For QoS reports, QoS monitoring policy must be enabled.
... enabled the periodic collection.	For any System Monitoring Periodic reports (CPU/Disk/Memory), the periodic collection must be enabled. Once enabled, the report must be generated after 12 hours to see the output.  <b>Note</b> Periodic collection can be enabled by clicking <b>Periodic Collection Enable</b> button under System Monitoring Setting in <b>https://&lt;Server IP&gt;/webacs/ncsDiag.do</b> .
... chosen the correct device type for a particular report.	Do not choose NCS devices for generating CE Performance reports as they are optical devices.
... selected the correct time period while generating a report.	You cannot choose a 2-week time period if you enabled the policy only 2 days ago.
... configured the device properly. For more details, see <a href="#">Configure Devices So They Can Be Modeled and Monitored, on page 34</a> .	For QoS reports, QoS must be configured/enabled on the device.
... successful device inventory collection. For more details, see <a href="#">Find Devices With Inventory Collection or Discovery Problems, on page 55</a>	For the reports to have data, the inventory collection status must be <b>Completed</b> .



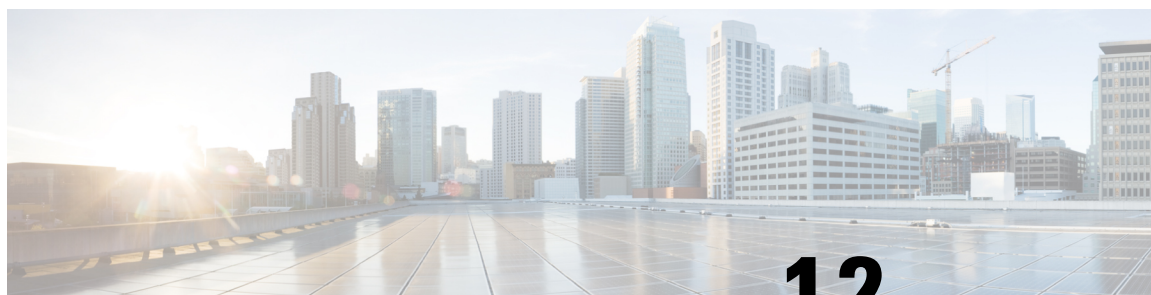
## PART **V**

# Configure Devices

- [Configure Devices, on page 267](#)
- [Create Templates To Automate Device Configuration Changes, on page 383](#)
- [Manage Cable Devices, on page 401](#)







## CHAPTER 12

# Configure Devices

---

This chapter provides the following topics:

- [Ways to Configure Devices Using Cisco Evolved Programmable Network Manager, on page 267](#)
- [Which Devices Support the Configuration Operations?, on page 268](#)
- [Identify the Commands Used In a CLI Configuration Template, on page 269](#)
- [Save Your Device Changes, on page 269](#)
- [Change a Device's Credentials and Protocol Settings, on page 270](#)
- [Change Basic Device Properties, on page 271](#)
- [Enable and Disable Interfaces, on page 272](#)
- [Configure Physical Attributes of Device Interfaces, on page 272](#)
- [Configure Circuit Emulation , on page 275](#)
- [Configure Alarm Profiles on Ports, Cards, and Nodes of Devices, on page 285](#)
- [Synchronize the Clock Using Sync-E, BITS, and PTP, on page 288](#)
- [Configure IP SLAs \(TWAMP Responder\), on page 293](#)
- [Configure Interfaces, on page 294](#)
- [Configure Devices Using the Chassis View, on page 320](#)
- [Configure Optical Cards, on page 331](#)
- [Discover and Configure MPLS LDP and MPLS-TE Links, on page 345](#)
- [Analyze Ports Using SPAN and RSPAN, on page 348](#)
- [Configure and View Ethernet Link Aggregation Groups , on page 350](#)
- [Configure Routing Protocols and Security, on page 352](#)
- [Configure EOAM Fault and Performance Monitoring, on page 362](#)
- [Configure Quality of Service \(QoS\) , on page 369](#)
- [Launch Cisco Transport Controller to Manage Cisco NCS and Cisco ONS Devices, on page 381](#)

## Ways to Configure Devices Using Cisco Evolved Programmable Network Manager

Cisco EPN Manager provides two ways to change the physical devices in your network. The actions you can perform depend on your user account privileges and the types of devices in your network.

Launch Points for Configuring Devices	Use this method to:
Configuration menu from left-side navigation menu	Perform common network management tasks on <i>one or more devices</i> using system templates—for example, adding a hostname or configuring a routing protocol. You can also create your own templates to fit your deployment needs. Because they can be applied to multiple devices, templates normally apply to specific device operating systems or device types. When you use a configuration template, Cisco EPN Manager only displays devices that meet the template criteria.
Manage device groups	By default, Cisco Evolved Programmable Network Manager creates dynamic device groups and assigns devices to the appropriate Device Type folder. You can create new device groups that appear under the User Defined folder.  Displayed in the left pane of the page.
View device details	Click on a <b>Device Name</b> to view the detailed configuration information for that device.  View device details such as memory, port, environment, and interface information.
Create and deploy configuration templates	Click on a <b>Device Name</b> , then click the <b>Configuration</b> tab.  You can configure device features on the selected device. You can also view the list of applied and scheduled feature templates that were deployed to the device.
View device configurations	Click on a <b>Device Name</b> , then click the <b>Inventory &gt; Device Management &gt; Configuration Archives</b> tab.  View archived configurations, schedule configuration rollbacks, and schedule archive collections.

**Note**

You can also edit device properties from the Network Devices table (**Configuration > Network > Network Devices**) by choosing a device and clicking **Edit**. This launches the device Edit Wizard. However, changes you make using the wizard are limited to device credentials, and any changes you make do not affect the physical device; they only update device information that is stored in the database.

For optical devices, you can also configure devices using Cisco Transport Controller, which you can launch from Cisco EPN Manager . See [Launch Cisco Transport Controller to Manage Cisco NCS and Cisco ONS Devices, on page 381](#)

After you make your changes, save your changes to the database and optionally collect the device's physical and logical inventory. For more information, see [Collect a Device's Inventory Now \(Sync\), on page 269](#).

## Which Devices Support the Configuration Operations?

Configuration operations are supported on a device if:

- The device model is supported by Cisco EPN Manager .
- The device operating system is supported by Cisco EPN Manager .

- The applicable technology or service is supported by Cisco EPN Manager *and* is enabled on the device.

To find out what is supported, see [Cisco Evolved Programmable Network Manager Supported Devices](#).

## Identify the Commands Used In a CLI Configuration Template

Use this procedure to view the exact commands that are used by any of the commands you launch from the **CLI Templates** drawer.

- 
- Step 1** Choose **Configuration > Templates > Features and Technologies**, then choose **CLI Templates**. For example:
- Out-of-the-box templates are under **System Templates - CLI**.
  - Customized templates are under **My Templates**.
- Step 2** Double-click the template in the left sidebar **Templates** menu.
- Step 3** In the Template Detail area, choose the **CLI Content** tab. The commands are displayed in that tab.
- 

## Save Your Device Changes

After you make a change to a device, save your changes to the database and, if desired, collect the device's physical and logical inventory. See these topics for more information:

- [Save Device Configuration Changes to the Database \(Update\)](#), on page 269
- [Collect a Device's Inventory Now \(Sync\)](#), on page 269

### Save Device Configuration Changes to the Database (Update)

After making a change to your devices, you should save those changes to the database by clicking **Update** in the configuration window. If an Update button is not provided, perform a manual *sync* which will save your changes, but also collect the device's physical and logical inventory and save it to the database. See [Collect a Device's Inventory Now \(Sync\)](#), on page 269

### Collect a Device's Inventory Now (Sync)

The Sync operation performs an immediate inventory collection for a device. When it performs a Sync, Cisco EPN Manager collects the selected device's physical and logical inventory and synchronizes the database with any updates. If you do not perform a Sync operation after making a change to a device, your change will not be saved to the database until the daily inventory collection.



**Note** The Sync operation is different from the Update operation. Update saves configuration changes without performing an inventory collection. If you want to use Update instead of Sync, see [Save Device Configuration Changes to the Database \(Update\)](#), on page 269.



**Note** This Sync operation is different from working with *out-of-sync device configuration files*. An out-of-sync device is a device that has a startup configuration files that is different from its running configuration file. For more information, see [Synchronize Running and Startup Device Configurations](#), on page 99.

Use one of these methods to perform a manual Sync.

To collect the inventory for:	Do the following:
A single device	<ul style="list-style-type: none"> <li>From the device's Device 360 view, choose <b>Actions</b> &gt; <b>Sync Now</b>.</li> <li>From the Network Devices table, check the device's check box, then click <b>Sync</b>.</li> </ul>
Multiple devices	From the Network Devices table, select the devices (by checking their check boxes), then click <b>Sync</b> .

## Change a Device's Credentials and Protocol Settings

Use the following procedure to update device credentials and protocol settings. When you save the settings to the database, you can also perform an inventory collection to gather all physical and logical device changes and save those changes to the database, rather than wait for the daily inventory collection.

- Step 1** Choose **Inventory** > **Network Devices**.
- Step 2** Select the device you want to edit, and click **Edit**. You can also choose several devices and make bulk changes.
- Step 3** Double-click the parameters you want to change. Depending on the device type, you can edit:
  - Credential profile being used by device
  - Group the device belongs to
  - SNMP port, retries, timeout, credentials, and SNMPv3 authentication information
  - Telnet/SSH2 credentials and timeout
  - HTTP/HTTPS credentials, port, timeout
  - IPSec parameters
  - TL1 credentials and proxy IP address (for GNE/ENEs)

**Step 4** Check that the new credentials are the same as those on the physical device by clicking **Verify Credentials**.

**Step 5** Save your changes:

- **Update** saves your changes in the database.
- **Update & Sync** saves your changes to the database, but also collects device physical and logical inventory and saves all changes to the database.

## Change Basic Device Properties

Cisco EPN Manager provides command templates that you can use to make basic property changes on your physical devices. To use these templates, choose **Configuration > Templates > Features & Technologies**, then choose **CLI Templates > System Templates – CLI** from the Templates pane on the left.



**Note** The operations you perform here are different from those you perform with the Edit wizard (which you can launch from the Network Devices table). The Edit wizard changes the device property information that is saved in the database. It does not change properties on physical devices.

CLI Configuration Template Name	Use it to:	Required Input Values
Add-Host-Name-IOS <i>and</i> -IOS-XR	Configure the client host name	Host name
Remove-Host-Name-IOS <i>and</i> -IOS-XR		
Syslog-Host-Logging-IOS <i>and</i> -IOS-XR	Specify host to which messages of a certain level will be logged	Host name
Add-Tacacs-Server-IOS <i>and</i> -IOS-XR	Configure the TACACS or TACACS+ server to use for authentication	Host address, key value, authentication list name, group name
Remove-Tacacs-Server-IOS <i>and</i> -IOS-XR		
Add-Tacacs-Plus-Server-IOS <i>and</i> -IOS-XR		
Remove-Tacacs-Plus-Server-IOS <i>and</i> -IOS-XR		
Add-SNMP-Configuration-IOS <i>and</i> -IOS-XR	Configure SNMP version, password, password encryption, server and group settings, UDP port, and so forth	Host name, community name
Remove-SNMP-Configuration-IOS <i>and</i> -IOS-XR		

CLI Configuration Template Name	Use it to:	Required Input Values
Enable-Traps-ASR903	Enable and disable traps on the Cisco ASR 903	Trap name (a list is provided)
Disable-Traps-ASR903		
Enable-Traps-IOS <i>and</i> -IOS-XR	Enable and disable traps on Cisco IOS and Cisco IOS XR devices	
Disable-Traps-IOS <i>and</i> -IOS-XR		
Enable-Traps-ME3600 <i>and</i> -ME3800	Enable and disable traps on the Cisco ME3600 and ME3800	
Disable-Traps-ME3600 <i>and</i> -ME3800		
Enable-Trap-Host-IOS <i>and</i> IOS-XR	Set a target host for SNMP traps	Host IP address, community string
Show-Users-on-Device-IOS and -IOS-XR	Display user session information for Cisco IOS and Cisco IOS XR devices	(Executed from selected device; no input required)

## Enable and Disable Interfaces

Use the Interface 360 view to quickly enable and disable an interface. While you can perform these same actions from a Device Details page, using the Interface 360 view may be more efficient (for example, when responding to an alarm). The top right of the Interface 360 view provides an **Actions** menu that provides enable and disable options.

To launch an Interface 360 view, see [Get a Quick Look at a Device Interface: Interface 360 View, on page 83](#).

To enable and disable an interface from a device's Device Details page, see the interface configuration topics (Ethernet, Loopback, Tunnel, and so forth).

## Configure Physical Attributes of Device Interfaces

Using Cisco EPN Manager, you can configure the physical attributes of your device's interfaces. Attributes such as card operating modes, bandwidth allocation per slot, slot pluggable types (such as VCoP), and AINS settings are configurable.

To configure the physical attributes of interfaces:

- 
- Step 1** Choose **Configuration > Network Devices**.
  - Step 2** Select the device that you want to configure by clicking the device's name hyperlink.
  - Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
  - Step 4** To configure the interfaces, navigate to the paths described in the table below.
  - Step 5** To make your changes, click the controller/card name hyperlink and click the Edit icon at the top right corner of the page. Make your changes and click **Save**.

Table 11: Physical Attributes Configuration for Interfaces

Physical Interface Configuration	Navigation	Comments/Descriptions	Supported Slots/Controllers
Configure card type as 5G or 10G.	<b>Physical &gt; Card Mode</b>	<p>You can change the configuration from 10G to 5G but the other way around is not supported. Depending on the device you select, the default card mode is set to either 5G or 10G. For mode detailed information on the supported card modes, see <a href="#">Supported Devices for Cisco EPN Manager</a></p> <p><b>Note</b> You cannot configure the card modes on slots that are part of active circuits.</p>	For more information about the device slots and supported card mode types, see table below ( <i>Device Slots and Supported Card Mode Types</i> ).
Configure card modes as T1 or E1.	<b>Physical &gt; Card Mode</b>	<p>You can change the configuration from T1 to E1 or vice versa depending on the device and card you select.</p> <p>T1 and E1 modes represent the type of channelization mode used on the card.</p> <p><b>Note</b> You cannot configure the card modes on slots that are part of active circuits.</p>	-
Configure card modes as OC3 or OC12.	<b>Physical &gt; Card Mode</b>	<p>You can set the card modes of A900-IMA4OS cards (of Cisco ASR 903 routers) as OC3 or OC12.</p> <p>OC3 and OC12 modes represent the data transmission rates on the different optical transmission lines.</p>	-
Configure Card Protection	<b>Physical &gt; Card Protection</b>	<p>Configure cards to act as primary or backup members (interfaces). A primary interface and its backup interface together make up a Protection Group (denoted by a unique integer). Associating cards with backup members ensures that when the primary interface fails, the protecting interface quickly assumes the traffic load from the primary interface. Cards displayed as the Active members are cards functioning as the protecting members of the service.</p> <p>Ensure that the Primary and Backup members are of the same type. For example, if you choose a T1 interface as a Primary member, the Backup member must also be a T1 interface.</p> <p>The Admin Mode for the protection group is configured in the order Lockout &gt; Force Switch &gt; Manual Switch &gt; None. For more information about these modes and the revert timer, see the descriptions in <a href="#">Configure APS and UPSR Protection Groups</a>, on page 279.</p>	-

Physical Interface Configuration	Navigation	Comments/Descriptions	Supported Slots/Controllers
Configure NCS4200-1T16G-PS cards on NCS42xx devices.	<b>Physical &gt; Card Mode</b>	You can view all the card modes of NCS4200-1T16G-PS cards, irrespective of the slot numbers.  <b>Note</b> Once you configure NCS4200-1T16G-PS card on some slots of NCS42xx devices, the configurations on those slots will be reset to the default values.	-
Configure A900-IMA8CT1Z-M and A900-IMA8CS1Z-M cards on ASR9xx devices.	<b>Physical &gt; Card Mode</b>	You can view and configure the card modes of A900-IMA8CT1Z-M and A900-IMA8CS1Z-M cards.	-
Configure the interface module type for Automatic In-Service (AINS)	<b>Physical &gt; Automatic In-Service (AINS)</b>	Use this menu to configure the right controller types for AINS.  In case of manual insertion and removal of cards, the AINS values are populated after a 20 min delay.	-
Configure bandwidth that must be reserved for the selected device slots.	<b>Physical &gt; Bandwidth</b>	The bandwidth you specify is reserved for the selected slot and made available to the slot irrespective of whether the slot is operational or not. In cases when the selected slot/card is down, and then back online after sometime, the configured bandwidth will be available for use based on the values specified in this field.	You can reserve a pre-configured bandwidth value of 80 or 100 Gbps on NCS4200-1T16G-PS cards on NCS42xx devices.
Configure the interface pluggable type for virtual Container over Packet (VCoP).	<b>Physical &gt; Pluggable Type</b>	Use this menu to select the right port types for VCoP enabled interfaces. For example, the port types can be OC3, OC12, or DS3.  <b>Note</b> VCoP smart SFP provides an ability to forward the SONET signal transparently across the packet network. The VCoP smart SFP is a special type of optical transceiver which encapsulates SONET bit stream at STS1 or STS-3c or STS-12c level into packet format.	-

**Conditions and Limitations:** Following are the conditions and limitations for configuring controller modes on Cisco ASR 900 Series Route Switch Processor 2 (RSP2A) modules (A900-RSP2A-128) that are supported on Cisco ASR 920, Cisco NCS4202, and Cisco NCS 4206 devices:

- The maximum bandwidth that can be configured is OC-48. A maximum of 20 ports on the module can be configured:
  - Ports 0-11 are T1 ports
  - Ports 12-15 are T3/E3 ports
  - Ports 16-19 are OC3/OC12 ports.



**Note** If a given port is configured as OC48, then only one of the given port can be configured since the maximum configurable bandwidth is OC48.

- Configuration limitations on the Cisco A900-RSP2A-128 modules:
  - You cannot configure SDH/E3/E1/DS0 controller modes.
  - Configuring Ethernet as the controller mode is not supported.
  - The protection type UPSR cannot be configured.
  - Once you deploy the controller mode configuration to the device, you cannot undo the configuration using Cisco EPN Manager .

**Table 12: Device Slots and Supported Card Mode Types**

Cisco NCS 4206 Devices	Cisco NCS 4216 Devices	Cisco ASR903 Devices	Cisco ASR907 Devices
<ul style="list-style-type: none"> <li>• Slot 0, 1 - Not supported</li> <li>• Slot 2, 3, 4, 5 - Default Mode 10G</li> </ul>	<ul style="list-style-type: none"> <li>• Slot 0, 1 - Not supported</li> <li>• Slot 3, 4, 7, 8, 11, and 12 - Default Mode 10G</li> <li>• Slot 2, 5, 6, 9, 10, 13, 14 and 15 - Default Mode 5G</li> </ul>	<ul style="list-style-type: none"> <li>• Slot 0, 1 - Not supported</li> <li>• Slot 2, 3, 4, 5 - Default Mode 10G</li> </ul>	<ul style="list-style-type: none"> <li>• Slot 0, 1 - Not supported</li> <li>• Slot 3, 4, 7, 8, 11, and 12 - Default Mode 10G</li> <li>• Slot 2, 5, 6, 9, 10, 13, 14 and 15 - Default Mode 5G</li> </ul>

**Table 13: Controller Modes and Supported Port Types**

Ethernet (0-7)	SONET (0-3)	SONET (4-7)
<ul style="list-style-type: none"> <li>• 8G (each 1G port)</li> <li>• Not allowed in a port group if at least one port has OC48 configured.</li> </ul>	<ul style="list-style-type: none"> <li>• Max of 2.5G</li> <li>• Can support OC48/OC12/OC3 but total of 2.5G</li> <li>• Example if Port 0 configured with OC48, Port1/2/3 can't be used.</li> </ul>	<ul style="list-style-type: none"> <li>• Max of 2.5G</li> <li>• If a port group has OC12/OC3/1G it means OC48 can't be allowed</li> </ul>

## Configure Circuit Emulation

Cisco EPN Manager supports the provisioning of Circuit Emulation (CEM) which provides a bridge between traditional TDM network and packet switched network (PSN). CEM is a way to carry TDM (or PDH) circuits over packet switched network. Circuit Emulation (CEM) is the imitation of a physical connection. This feature allows you to use your existing IP network to provide leased-line emulation services or to carry data streams or protocols that do not meet the format requirements of other multiservice platform interfaces.

Cisco EPN Manager supports the following CEM modes:

- Structure-Agnostic time-division multiplexing (TDM) over Packet (SAToP)—This is the unstructured mode in which the incoming TDM data is considered as an arbitrary bit stream. It disregards any structure that may be imposed on the bit stream. SAToP encapsulates the TDM bit streams as pseudowire (PWs) over PSN.
- Circuit Emulation over Packet (CEP)—This mode is used to emulate Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) circuits and services over MPLS. To transport SONET/SDH circuits through a packet-oriented network, the Synchronous Payload Envelope (SPE) or Virtual Tributary (VT) is broken into fragments. A CEP header and optionally an RTP header are prepended to each fragment.

For more information about CEM in Cisco EPN Manager, see, [Supported Circuit Emulation Services, on page 425](#).

When a line is channelized, it is logically divided into smaller bandwidth channels called higher-order paths (HOP) and lower-order paths (LOP). These paths carry the SONET payload. When a line is not channelized, the full bandwidth of the line is dedicated to a single channel that carries broadband services. Cisco EPN Manager enables you to channelize the T3 or E3 channels into T1s, and channelize the T1s further into DS0 time slots. Before you provision CEM services using Cisco EPN Manager, you must first configure the parameters for the HOP and LOP by configuring the interfaces for CEM.

A channelized SONET interface is a composite of STS streams, which are maintained as independent frames with unique payload pointers. The frames are multiplexed before transmission. SONET uses Synchronous Transport Signal (STS) framing while SDH uses Synchronous Transport Mode (STM) framing. An STS is the electrical equivalent to an optical carrier 1 (OC-1) and an STM-1 is the electrical equivalent to 3 optical carrier 1s (OC-1s).

This section describes how you can use Cisco EPN Manager to first configure your interfaces for CEM. You can then provision CEM services using these interfaces configured with appropriate controller modes and protection groups.

## Pre-requisites for Configuring CEM Services

Before you provision a CEM service (see [Provision Circuit Emulation Services, on page 483](#)), ensure that the following pre-requisites are met:

- Configure the required loopback settings for CEM on the device. See, [Configure Loopback Interfaces, on page 296](#).
- Configure the required CEM parameters on SONET, SDH, PDH, HOP, and HOP controllers. See, [Configure Interfaces for CEM, on page 276](#).
- Configure the working and backup interface groups to provide APS protection. See, [Configure APS and UPSR Protection Groups, on page 279](#).

## Configure Interfaces for CEM

Using Cisco EPN Manager, you can configure your interfaces with Circuit Emulation (CEM). To do this, you must first set appropriate controller modes on your interfaces and then configure the PDH (E1, T1, E3, T3), SONET, and SDH controllers for CEM. After you configure the interfaces with CEM, you can then use the interfaces for provisioning CEM services. See [Provision Circuit Emulation Services, on page 483](#).

To configure the interfaces for CEM:

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Select the device that you want to configure by clicking the device's name hyperlink.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** To configure CEM parameters, navigate to the configuration options as described in the table below.
- Step 5** To make your changes, click the controller/card name hyperlink and click the Edit icon at the top right corner of the page. Make your changes and click **Save**.
- 

### Example

*Table 14: CEM Interface Configuration Options*

CEM Interface Configuration	Navigation	Comments	Supported Slots/Controllers
Configure controller modes as SONET, SDH, Ethernet, T3, or E3.	<b>Circuit Emulation &gt; Controller Mode</b>	The controller mode options displayed for selection are based on the selected media type.	—
Configure PDH (E1, T1, E3, and T3) controllers	<b>Circuit Emulation &gt; PDH</b>	For a description of the different PDH parameters, see <a href="#">CEM Interface (PDH, SONET, and SDH) Field Descriptions</a> , on page 282	-

CEM Interface Configuration	Navigation	Comments	Supported Slots/Controllers
Configure SONET and SDH controllers for CEM	<b>Circuit Emulation &gt; SONET and SDH</b>	For a description of the different SONET and SDH parameters, see <a href="#">CEM Interface (PDH, SONET, and SDH) Field Descriptions</a> , on page 282	For more information about the device ports and supported controller types, see table below ( <i>Controller Modes and Supported Port Types</i> ).
Configure a working and protecting member interface for CEM provisioning.	<b>Circuit Emulation &gt; Protection Group</b>	See <a href="#">Configure APS and UPSR Protection Groups</a> , on page 279	-

Table 15: Controller Modes and Supported Port Types

Ethernet (0-7)	SONET (0-3)	SONET (4-7)
<ul style="list-style-type: none"> <li>• 8G (each 1G port)</li> <li>• Not allowed in a port group if at least one port has OC48 configured.</li> </ul>	<ul style="list-style-type: none"> <li>• Max of 2.5G</li> <li>• Can support OC48/OC12/OC3 but total of 2.5G</li> <li>• Example if Port 0 configured with OC48, Port1/2/3 can't be used.</li> </ul>	<ul style="list-style-type: none"> <li>• Max of 2.5G</li> <li>• If a port group has OC12/OC3/1G it means OC48 can't be allowed</li> </ul>

**CEM Interface Configuration Example:**

The following example show the sample CEM interface configuration that is deployed to the device for CEM framing type 'unframed', c-11 mode, clock source of type 'internet', and ACR values associated with the Protection Group 'acr 255':

```
NCS4206-120.32#show running-config | section 0/4/0
controller MediaType 0/4/0
 mode sonet
controller SONET 0/4/0
 rate OC3
 no ais-shut
 framing sonet
 clock source line
 loopback network
 !
 sts-1 1
```

```

clock source internal
mode unframed
cem-group 1 cep
!
sts-1 2
clock source internal
loopback network
mode unframed
cem-group 2 cep
!
sts-1 3
clock source internal
mode vt-15
vtg 1 vt 1 protection-group 15 working
vtg 1 vt 3 protection-group 16 working
vtg 1 vt 4 protection-group 17 working
!
aps group acr 255
aps protect 1 6.6.6.6 / aps working 1
!
interface CEM0/4/0
no ip address
cem 1
!
cem 2
!
connect sam CEM0/4/0 1 CEM0/4/0 2
!
NCS4206-120.32#

```

## Configure APS and UPSR Protection Groups

Viewing the protection groups for CEM helps you understand the enabled Automatic Protection Switching (APS) and Unidirectional Path Switched Ring (UPSR) interfaces for your devices. APS and UPSR refers to the mechanism of using a protect interface in the SONET network as the backup for the working interface. Associating your interfaces with APS or UPSR protection groups, ensures that when the working interface fails, the protect interface quickly assumes its traffic load. The working interfaces and their protect interfaces together make up a Protection Group. SONET Protection Groups offer recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer. Using Cisco EPN Manager , you can view the working member for a SONET controller which acts as the main functioning controller for the CEM circuit. The Protecting Member acts as a backup for the main working controller. To view these details, ensure that the interfaces have been set with the required controller modes as explained in [Configure Interfaces for CEM, on page 276](#).

To configure APS protection groups and view UPSR interfaces:

- 
- Step 1** Choose **Configuration > Network Devices**.
  - Step 2** Select the device that is configured with protection groups, by clicking the device's name hyperlink.
  - Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
  - Step 4** Choose **Circuit Emulation > Protection Group**.
  - Step 5** To configure the APS parameters, click the **APS** tab, click the Protection Group hyperlink of the group that you want to modify, and click the Edit icon at the top right corner of the page.
  - Step 6** You can view and configure the following fields.

- The **Working Member** represents the SONET controller which acts as the main functioning controller for the circuit.
- The **Protecting Member** represents the SONET controller which acts as the backup to the working member for the circuit.
- The **Protection Status** indicates whether the group is an active or inactive member for the circuit.
- The **Hello Time** and **Hold Time** fields represent the time range for the protecting and working members. The hello timer defines the time between hello packets. The hold timer sets the time before the protect interface process declares a working interface's router to be down. By default, the hold time is greater than or equal to three times the hello time.
- The **Loopback IP** determines the configuration for the protect interface which includes the IP address of the router (normally its loopback address) that has the working interface.
- The **Revertive Time**, in minutes, enables automatic switchover from the protect interface to the working interface based on the configured time after the working interface becomes available.
- The **Directional** drop-down menu represents the direction in which the backup protection must be enabled.
  - In the bidirectional mode, a failure on a working member triggers an APS switchover of the working member to the Protecting member. Here the receive and transmit channels are switched as a pair.
  - In the unidirectional mode, failure on a working member triggers an APS switchover of only the failed member to the corresponding line of the Protection interface.
- The **ADM** checkbox, if enabled, associates Add Drop Multiplexors (ADMs) with the protecting member.
- The **APS Request** drop-down menu enables you to configure the following values. The values can be configured in the order Lockout > Force Switch > Manual Switch > No Mode. For example, if Force Switch is currently configured on the device, then you can configure only Manual Switch or No Mode values. You cannot configure Lockout when Force Switch is configured.
  - **Lockout:** Prevents a working interface from switching to a protect interface. For example, if the protect interface is configured as circuit 1, the Lockout option prevents the protect interface from becoming active.
  - **Manual Switch:** Manually switches a circuit to a protect interface, unless a request of equal or higher priority is in effect.
  - **Force Switch:** Manually switches a circuit to a protect interface, unless a request of equal or higher priority is in effect. For example, if the protect interface is configured as a particular circuit, the force command sets the protect interface to active.
  - **No Mode:** Removes the current APS request configuration from the protection group on the device.

**Step 7** To view similar parameters associated with UPSR interfaces, click the **UPSR** tab.

You can view information such as the protection group number, working and protecting members configured on the device, the active paths for the group, and its current protection status. This information cannot be modified.

### What to do next

To delete the APS configuration on your devices, you must first shutdown the controller by setting the Admin Status field (under the SONET and SDH menu) to Down. Then, return to the Protection Group menu to delete the required APS configuration.

## Configure Clocking for CEM

Clocking modes define multiple ways to achieve the same clock in the transmitting and receiving ends of a CEM circuit. Cisco EPN Manager enables you to configure clock recovery and distribution in these ways:

- **Synchronous Clocking** — with synchronous clocking, PDH (TDM) lines on the source and destination are synchronized to the same clock delivered by some means of physical clock distribution (SONET, SDH, and so on). The clock on the particular TDM line can be delivered from
  - **Line:** the transmit clock is from the receiver of the same physical line.
  - **Internal:** the controller will clock its sent data using the internal clock.
  - **Free Running:** the transmit clock is taken from line card and can be derived from an internal free running oscillator.
  - **Recovered:** the transmit clock is derived from an in-band pseudowire-based activeclock recovery on a CEM interface.

To set these clocking values in Cisco EPN Manager, see [Configure CEM Interfaces](#).

- **Adaptive Clocking** — adaptive clocking is used when the routers do not have a common clock source. The clock is derived based on packet arrival rates based on dejitter buffer fill level. You can set the size of the Dejitter Buffer (in the range of 1-32) during provisioning of CEM services in Cisco EPN Manager. The size of the Dejitter Buffer determines the ability of the circuit to tolerate network jitter.
- **Differential clocking** — differential clocking is used when the cell site and aggregation routers have a common clock source but the TDM lines are clocked by a different source. The TDM clocks are derived from differential information in the RTP header of the packet with respect to the common clock. Differential clock recovery is based on time stamps received in the RTP header.

To configure clock recovery for CEM:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Click the <b>Configuration</b> tab, then click the <b>Logical View</b> left side tab.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 2</b> | Choose <b>Clock &gt; Recovered Clock</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 3</b> | To add a new interface from which the clock source must be derived, click the Add ('+') icon.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 4</b> | To edit the existing recovered clock configuration, click the Recovering Interface hyperlink and click the 'Edit' icon at the top right of the page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 5</b> | Specify the following recovered clock values: <ol style="list-style-type: none"><li>1. Enter a unique numerical value for the <b>Recovered Clock ID</b> for easy identification of the recovered clock configuration. This ID can then be used to associate the CEM interfaces directly with this the recovered clock configuration.</li><li>2. From the <b>Recover Mode</b> drop-down list choose:<ul style="list-style-type: none"><li>• <b>Adaptive</b>— when devices do not have a common clock source, the recovered clock is derived from packet arrival rate on the controller selected as the Protecting Member for the associated Protection Group.</li></ul></li></ol> |

- **Differential**— when the edge devices have a common clock source, the recovered clock is derived from timing information in packets and the related difference from the common clock.

3. Enter a unique numerical value for easy identification of the **CEM Group Number**. This identifies the CEM group associated with the clock.
4. Choose the required controller from the **Recovering Interface** drop-down list. This controller associated with the clock is the virtual CEM interface from which the clock is derived when a backup clock source is required.

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

Your changes are saved and deployed to the device.

## CEM Interface (PDH, SONET, and SDH) Field Descriptions

To configure the CEM parameters listed in the table below:

**Step 1** Configure the required CEM parameters on SONET, PDH, HOP, and HOP controllers. See, [Configure Interfaces for CEM, on page 276](#).

**Step 2** Configure clock distribution and recovery for CEM. See [Configure Clocking for CEM, on page 281](#).

**Table 16: Table - CEM Interface (SONET, SDH, and PDH) Field Descriptions**

Fields	Descriptions	Values	Descriptions	Applicable Controller Modes
Rate	Identifies the rate at which the bit-transparent data transport occurs. It is defined by the CEoP Shared Port Adapters (SPA) group that you choose.	LR_DSR_OC3_STM1	Indicates the layer rate supported on the channelized OC-3 line with STM level 1. OC-3 is an optical carrier network line with transmission data rate of up to 155.52 Mbit/s.	SONET
		LR_DSR_OC12_STM4	Indicates the layer rate supported on the channelized OC-12 line with STM level 4. OC-12 is an optical carrier network line with transmission data rate of up to 622.08 Mbit/s.	SONET
		LR_DSR_OC48_STM16	Indicates the layer rate supported on the channelized OC-48 line with STM level 16. OC-48 is an optical carrier network line with transmission data rate of up to 2.4Gbps.	SONET
		LR_DSR_OC192_STM64	Indicates the layer rate supported on the channelized OC-192 line with STM level 64.  A channelized OC-192 line with STM level 64. OC-192 is an optical carrier network line with transmission data rate of up to 9.6Gbps.	SONET



Fields	Descriptions	Values	Descriptions	Applicable Controller Modes
Mode	Identifies the type of channelization, such as Synchronous Transport Signal of level n (STS-n), for high-order and low-order paths.	High- Order Path values: STS3C, STS12C, STS48C, STS192C, T3, UNFRAMED, VT15, VT2, CT3, and CT3_E1.  Low Order Path values: VT15, T1, and E1.	<ul style="list-style-type: none"> <li>• STS-n: Mode with Synchronous Transport Signal (STS) channelization of level n.</li> <li>• T1, E1, T3, and E3: Indicates the channelization mode used on the controller. T1 or E1 circuit has a transmission data rate of up to 1.544 Mbit/s. The T3 or E3 circuit has a transmission data rate of up to 44.736 Mbit/s.</li> <li>• VT 1.5: Indicates that the controller is a virtual tributary network line with transmission data rate of up to 1.728 Mbit/s.</li> <li>• VT 2: Indicates that the controller is a virtual tributary network line with transmission data rate of up to 2.304 Mbit/s.</li> <li>• Unframed: indicates that a single CEM channel is used for all T1/E1 timeslots.</li> </ul>	HOP and LOP.
Clock Source	Identifies the source of the clock signal sent on SONET ports.	Line	Controller will clock its sent data using the clock recovered from the line's receive data stream.	All
		Internal	The transmit clock is taken from line card and can be derived either from an internal physical line.	All
		Free-Running	The transmit clock is taken from line card and can be derived from an internal free running oscillator.	All
		Recovered	In-band pseudowire-based activeclock recovery on a CEM interface which is used to drive the transmit clock.	SONET, HOP, and LOP.
		Enhanced	-	SONET, HOP, and LOP.

Fields	Descriptions	Values	Descriptions	Applicable Controller Modes
Framing	Framing mode used for the CEM channel.	CRC and NO_CRC.	CRC: represents the framing type with cyclic redundancy check.	SONET
		Unframed, DSX1_ESF, DSX1_SF, Auto Detect, C_BIT, and M23.	<ul style="list-style-type: none"> <li>Unframed: indicates that a single CEM channel is used for all timeslots.</li> <li>DSX1_SF: indicates that the DS1 type of interface has the framing type as super frame. SF uses 12 frames per super frame for in-band signaling extraction.</li> <li>DSX1_ESF: indicates that DS1 type of interface has the framing type as extended super frame. ESF uses 24 frames per ESF.</li> </ul>	PDH, HOP, and LOP.
Loopback	Specifies the loopback value associated with the CEM interface.	Local, Network Line, Remote, Remote Line, Network Payload, and Unknown.	For a detailed explanation about the different loopback values, refer the latest IOS Command References.	All
		Diag, Local Payload, Remote ESF Payload, Remote ESF Line, Remote ESF Line CSU, Remote ESF Line NIU, Remote Iboc, Remote Iboc CSU, Remote Iboc FAC1, Remote Iboc, and FAC2.	—	PDH
Protection Role	Identifies the priority based on which the recovered clock must be obtained.	Primary	The recovered clock is obtained from a clock with the highest priority.	SONET
		Secondary	The recovered clock is obtained from a clock with a lower priority than the primary clock.	SONET
Cable Length	Sets the transmission attenuation according to the length of the cable. For example, if you choose short 115, the cable length is from 0 to 115 feet. Choose Short 220 if the cable length is from 110 to 220 feet, and so on. Your values are between Short 110 to Short 550, Shot LT 225, and Long GT 225.			PDH
Line Coding	Line encoding method for the controller: <ul style="list-style-type: none"> <li>For E1, the options is Alternate Mark Inversion (AMI).</li> <li>For T1, the options are AMI and bipolar with 8 zero substitution (B8ZS).</li> </ul>			PDH

Fields	Descriptions	Values	Descriptions	Applicable Controller Modes
Channelization Mode	Indicates the channelization mode that must be used on the controller. A T1 or E1 circuit has a transmission data rate of up to 1.544 Mbit/s. Your values are T1, E1, and Unchannelized.			PDH
Protection Group Number	Identifies the group number associated with the clock for the CEM interface.			SONET
Protection Loopback Name	Identifies the loopback group number associated with the clock for the CEM interface.			SONET
Protection Loopback IP	Identifies the IP address of the loopback interface associated with the CEM interface.			SONET
Protection Revertive Time	Identifies the backup revertive time settings associated with the clock for the CEM interface.			SONET
Operational Status	Operational status of the CEM interface. This field cannot be edited.	Up, Down, and Not-Applicable.	<ul style="list-style-type: none"> <li>• Down— the interface is down.</li> <li>• Not-Applicable— the interface has an unknown operational status.</li> <li>• Up— the interface is up.</li> </ul>	SONET, HOP, and LOP.
Admin Status	Administrative status of the CEM interface.	Up, Down, and Not-Applicable.	<ul style="list-style-type: none"> <li>• Up— the CEM interface is administratively up.</li> <li>• Down— the CEM interface is administratively down.</li> <li>• Not-Applicable— the administrative status is unknown.</li> </ul>	SONET, HOP, and LOP.
Recovered Clock ID	Unique identifier for the clock settings associated with the CEM interface. To configure the Recovered Clock ID, see Configure Clocking for CEM.			PDH, HOP, and LOP.

## Configure Alarm Profiles on Ports, Cards, and Nodes of Devices

The Alarm Profiles feature allows you to change default alarm severities by creating unique alarm profiles for different interfaces of the device. An Alarm Profile applied to one node on the network cannot be applied to other nodes using Cisco EPN Manager . When you create Alarm Profiles, they are first stored on the node before they can be applied to the node, card, or port (using the Alarm Behavior menu). The Alarm Behavior menu displays the alarm profiles saved on the selected device.

In the Node view, the Alarm Behavior tab displays the alarm profiles for the node. Alarms form a hierarchy. A node-level alarm profile applies to all cards in the node, except those that have their own profiles. A card-level alarm profile applies to all ports on the card, except those that have their own profiles. At the node level, apply profile changes on a card-by-card basis or set a profile for the entire node. At the card level, apply profile changes on a port-by-port (module) basis or set the profiles for all ports on that card simultaneously (using the Port Profiles tab).




---

**Note** If an Alarm Profile is applied to a node, it cannot be applied to the cards and ports associate with the same node. And if it is applied to the card, it cannot be applied to the ports associate with the same card.

---

To create alarm profiles and associate them with interfaces:

---

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab, then click the left side **Logical View** tab.

**Step 4** Create new alarm profiles with severity parameters:

- a) Choose **Alarm > Alarm Profile**.
- b) To add a new alarm profile, click the '+' button.
- c) Specify a unique name for the alarm profile and click **Save**.  
The name cannot contain special characters or the words 'Default' and 'SupressAlarm'.
- d) To associate alarm severity parameters to the alarm profile created in the step above:
  1. Locate the alarm profile from the Alarm Profiles list, by clicking the Alarm Name hyperlink.
  2. Click the **Profile Details** tab.
  3. Click the '+' icon to add a new set of severity parameters, and to edit existing severity parameters, click the appropriate Condition hyperlink and then click the Edit icon at the top right corner of the page .
- e) Specify the following severity parameters:

**Note** You can associate only a single alarm profile to a given interface. However, the same alarm profile may be associated with multiple interfaces.

Table 17:

Fields	Applicable Values	Descriptions
Alarm Type	-	The type of alarm for which the specified conditions must be met. Select one of these options: <ul style="list-style-type: none"> <li>• HW_Optics</li> <li>• HW_Ehternet</li> <li>• HW_GFP</li> <li>• HW_G709</li> <li>• HW_SONET</li> <li>• HW_SDH_Controller</li> </ul>
Service Affecting Severity	Critical	The alarm is a critical, traffic-affecting alarm.
	Major	The alarm is a major alarm.
Non Service Affecting Severity	Minor	The alarm is a minor alarm.
	Not Alarmed	A raise or clear of the condition is sent to clients as a nonalarmed TL1 message (REPT EVT). The message has no severity and no service affecting flag.
	Not Reported	A raise or clear of the condition is not sent to clients, but is tracked on the NE.
	Default	Indicates the default device severity value.
Condition	-	The type of condition that must be considered for the Alarm Type selected above.

At this stage the profile is created and pushed to the device. For alarm profiles to be activated, you need to apply this alarm profile to the required nodes/cards/ports as explained in the steps below.

**Step 5**

Apply the alarm profile to the device:

- Choose **Alarm > Alarm Behavior**.
- Click the '+' sign to configure the alarm behavior parameters.

**Note** Before you apply an alarm profile to an interface, ensure that the interface has not inherited the same alarm profile from its parent. This could cause the application of the alarm profile to fail.

- Depending on the type of interface that you want to apply the alarm profile to, click on the **Node Profiles**, **Card Profiles**, or **Port Profiles** tabs.
- Depending on the interface that you want to apply the alarm profile to, click on the appropriate Alarm Profile Name hyperlink and then click the Edit icon at the top right corner of the page.
- Use the **Alarm Profile Name** drop-down menu to choose the alarm profile that must be applied to this interface.
- Use the **Suppress Alarm** checkbox to specify whether or not the alarms for a particular card/node/port must be suppressed. If checked, all generated alarms are suppressed.

- g) Click **Save** to deploy your changes to the device. The profile you created is now applied to the specified ports/cards/nodes.

Once an alarm profile has been applied to an interface, the alarm profile cannot be deleted from Cisco EPN Manager. To delete the alarm profile you need to ensure that its association with the interfaces has been removed.

- h) (Optional) Navigate to **Monitor > Monitoring Tools > Alarms and Events** to access the Alarms Table that shows all alarms for all devices, for a specific device group, or for a specific device. You may need to wait until the devices sync before you can view the generated alarms.

## Synchronize the Clock Using Sync-E, BITS, and PTP

### Synchronous Ethernet (Sync-E):

Using Cisco EPN Manager, you can enable frequency synchronization to provide high-quality bit clocks synchronization over Ethernet interfaces. Synchronous Ethernet (Sync-E) provides this required synchronization at the physical level.

To do this you need to configure Sync-E that helps routers identify the clock in the network with the highest priority. This clock is also called the Master Clock. All the other devices (members) on the network reset their clocks based on the master clock's settings. Messages are constantly exchanged between the master clock and its members to ensure efficient continued synchronization of all clocks in the network. Cisco EPN Manager enables you to specify this master clock and also set the Sync-E parameters at the global and interface levels. Once the Sync-E properties have been configured, you can view the logical hierarchy and topology between the devices on the network topology overlay.



**Note** Sync-E configuration is supported only on Ethernet interfaces.

### Building Integrated Timing Supply (BITS):

BITS is the method by which clocking information is provided by a Building Integrated Timing Supply (BITS) port clock. In Sync-E, Ethernet links are synchronized by timing their bit clocks from high-quality, stratum-1-traceable clock signals in the same manner as SONET/SDH. Operations messages like SSM and ESMC maintain Sync-E links and ensure that a node always derives its timing from the most reliable source.

### Precision Time Protocol (PTP):

In networks that employ TDM, periodic synchronization of device clocks is required to ensure that the receiving device knows which channel is the right channel for accurate reassembly of the data stream. The Precision Time Protocol (PTP) standard:

- Specifies a clock synchronization protocol that enables this synchronization.
- Applies to distributed systems that consist of one or more nodes communicating over a network.

PTP uses the concept of master and slave devices to achieve precise clock synchronization. With the help of Cisco EPN Manager, you can use PTP to configure the master device which periodically starts a message exchange with the slave devices. After noting the times at which the messages are sent and received, each slave device calculates the difference between its system time and the system time of the master device. The slave device then adjusts its clock so that it is synchronized with the master device. When the master device

initiates the next message exchange, the slave device again calculates the difference and adjusts its clock. This repetitive synchronization ensures that device clocks are coordinated and that data stream reassembly is accurate. The PTP clock port commands are used to modify PTP on individual interfaces. Once the PTP properties have been configured, you can view the logical hierarchy and topology between the devices on the network topology overlay.



**Note** Due to the limitations on the device, you can configure a maximum of 4 clock sources on interface modules, with a maximum of 2 per interface module. This limitation applies to both Sync-E and TDM interfaces.

To configure Sync-E, BITS, and PTP:

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Select the device that you want to configure by clicking the device's name hyperlink.
- Step 3** Set the global Sync-E properties.
- Click the **Configuration** tab, then click the **Logical View** left side tab.
  - Click **Clock > Sync-E**. All available Sync-E global settings are listed.
  - To create a new set of global Sync-E properties, click the '+' icon. You can create only one set of Sync-E global parameters.
  - Specify the global parameters for Sync-E. For a detailed description about these parameters, see the table below.
  - Click **Save**.  
Your changes are saved and the global Sync-E configuration is deployed to the device. You can now specify the interfaces that you want to associate with this configuration.
- Step 4** Specify the associated interfaces and interface specific Sync-E parameters.
- Select the Sync-E global configuration created in the above steps from **Clock > Sync-E**.
  - Click the **Interface Input Source** tab.
  - Click '+' to specify the required interfaces.  
You can configure only one interface per synchronization type.
  - Use the **Interface Name** drop-down menu to select the required interface.
  - Specify the interface level Sync-E parameters. For a detailed description about these parameters, see table below.
  - Click **Save**.
- Step 5** Specify the frequency settings for BITS:
- Click the **Configuration** tab, then click the **Logical View** left side tab.
  - Click **Clock > BITS-Frequency**.
  - Specify the following BITS values:
    - Source slot: Your options are RO and R1.
    - Priority: Enter a numeric value within the range 1 to 250.
    - Clock Type: Your options are E1 and T1.
  - Click **Save**.
  - Specify the BITS clock settings for the interface:
    - Navigate to **Clock > BITS-Frequency** and select the BITS Frequency settings created in the above step.

2. Click the **Bits Clock Settings** tab and specify the clock settings as described in the table below.
3. Click **Save**.

**Step 6** Specify the interface settings for BITS:

- a) Click the **Configuration** tab, then click the **Logical View** left side tab.
- b) Click **Clock > BITS-Interface**.
- c) Specify the following BITSs values:
  - **Source slot:** The values are RO and R1.
  - **Priority:** Numeric value within the range 1 to 250.
  - **Clock Type:** The values are 2.048MHz and 10MHz.

- d) Click **Save**.

Your changes are saved and the selected interfaces are associated with the Sync-E parameters. To verify your changes view the Sync-E and BITS parameters under **Configuration** tab > **Clock** for the selected device.

**Step 7** Specify the PTP clock settings:

- a) Click the **Configuration** tab, then click the **Logical View** left side tab.
- b) Click **Clock > PTP**.
- c) Click '+' to specify a new set of PTP values, or click the Clock Mode hyperlink and then click the Edit icon at the top right corner of the page.
- d) Specify the following common PTP parameters and click **Save**.
  - **Clock Mode:** Choose the mode of PTP operation. Your options are **Ordinary**, **Boundary**, and **E2E Transparent**. E2E stands for End-to-end transparent clock mode.
  - **Domain No:** Enter the number of the domains used for PTP traffic. A single network can contain multiple domains. Range is from 1 to 127.
  - **Hybrid Clock:** Enable or disable hybrid cloud.
- e) Click the Clock Mode hyperlink and click the **Port** tab to specify the port details that must be associated with the common properties.
- f) Specify the following Port details and click **Save**.
  - **Port Name:** Enter the name of the PTP port clock.
  - **Port Mode:** Choose the PTP role of the clock, Master or Slave.
  - **Loopback Interface Number:** Enter the clock identifier derived from the device interface.
  - **Announce Timeout:** Enter the number of PTP announcement intervals before the session times out. Range is 1 to 10.
  - **Delay Request Interval:** Choose the time when the interface is in PTP master mode and the selected interval is specified to member devices for delay request messages. The intervals use base 2 values.
  - **Sync Interval:** Choose the time interval for sending PTP synchronization messages.
  - **Announce Interval:** Choose the time interval for sending PTP announcement packets.
- g) Click the Port Name hyperlink and click the **Clock Source** tab.



- h) Click '+' to add a new interface, or click the source address hyperlink and click Edit at the top right corner of the page.
- i) Specify the **Source Address** and the **Priority** for the clock.
- **No Priority**- Assigns the priority value as 0.
  - **Priority 1**- Checks the first value for clock selection. The clock with the lowest priority takes precedence and the value 1 is assigned.
  - **Priority 2**- If two or more clocks have the same value in the Priority 1 field, the value in this field is used for clock selection. This assigns the priority value of 2.
- j) Click **Save** to deploy your changes to the device.

For detailed descriptions about all Sync-E global and interface level parameters, see the table below:

Fields	Descriptions
<b>Clock &gt; Sync-E Common Properties (Global Level)</b>	
Synchronous Type	Indicates the type of method used for synchronization of the clocks. The values are: Automatic, Forced, Manual, and Cisco. Note- You can configure only one interface per synchronization type.
Clock Type	Indicates the Ethernet Equipment Clock (EEC) option to be used: Option 1- represents EEC-Option I of the European time zone. Option 2- represents EEC-Option II of the American time zone.
QL Mode Enabled	Indicates whether the clock is to be used with the Quality Level (QL) function: Enabled or Disabled.
ESMC Enabled	Indicates the status of the Ethernet Synchronization Message Channel (ESMC): Enabled or Disabled.
SSM Option	Indicates the Synchronization Status Message (SSM) option being used: Option 1- represents ITU-T Option I Option 2- GEN1- represents ITU-T Option II Generation 1 Option 2- GEN2- represents ITU-T Option II Generation 2
Hold Off Time (global level)	Indicates the length of time (in milliseconds) for a device to wait before issuing a protection response to a failure event. A valid range is between 300 and 1800 milliseconds.
Wait To Restore Time (global level)	Indicates the length of time (in seconds) to wait after a failure is fixed before the span returns to its original state. A valid range is between 0 and 86400 seconds.
Revert Enabled	Specifies whether the network clock is to use Revertive mode: Enabled or Disabled.
<b>Sync-E &gt; Interface Input Source (Interface Level) Properties</b>	

Fields	Descriptions
Interface Name	Name and hyperlink of the Gigabit or 10 Gigabit interface associated with Sync-E.
Active clock	Indicates whether the interface is currently chosen as the active clock. This interface can either be a primary or secondary interface, however, the interface that is currently enabled for Sync-E is considered to be the active interface.
Priority	Indicates the value used for selecting a Sync-E interface for clocking if more than one interface is configured. Values are from 1 to 250, with 1 being the highest priority.  The highest priority clock represents the master clock.
Hold Off Time (interface level)	Indicates the length of time (in milliseconds) to wait after a clock source goes down before removing the source.  A valid range is a value between 300 and 1800 milliseconds.
Wait To Restore Time (interface level)	Indicates the length of time (in seconds) to wait after a failure is fixed before the interface returns to its original state.  A valid range is a value between 0 and 86400 seconds.
Rx Exact/QL Use	Indicates the QL Receive function with which the clock must be used.
Tx Exact/QL Send	Indicates the QL Transmit function with which the clock must be used.
<b>Clock &gt; BITS-Frequency and BITS-Interface Properties</b>	
Source Slot	Indicates whether the clock source is R0 or R1.
Priority	Indicates the value used for selecting a BITS interface for clocking if more than one interface is configured. Values are from 1 to 250, with 1 being the highest priority.  The highest priority clock represents the master clock.
Clock Type	Indicates whether the clock type that must be used is from an E1 line or a T1 line.  In case of the Bits Interface parameters, the clock type indicates the frequency values that must be associated with the clock. The options are 2.048MHz and 10MHz.
Bits Framing	Framing values (such as CAS) that must be associated with the BITS configuration.
Impedance	The impedance value that is associated with the clock in OHMS format. The default value is 120 ohms.

Fields	Descriptions
Line code	Line encoding method for the DS1 link: <ul style="list-style-type: none"><li>• For E1, the options are Alternate Mark Inversion (AMI) and high-density bipolar of order 3 (HDB3).</li><li>• For T1, the options are AMI and bipolar with 8 zero substitution (B8ZS).</li></ul>

### What to do next

(Optional) You can view the Sync-E and PTP device properties on the network topology overlay. See [Show Clock Synchronization Networks on a Network Topology Map, on page 172](#):

- **Sync-E overlay**: shows the topology and hierarchy of the Sync-E network. It shows the primary clock and the primary and secondary clock inputs for each device.
- **PTP overlay**: shows the clock synchronization tree topology, the hierarchy of the Precision Time Protocol, and the clock role of each device in the tree (master, boundary, slave, or transparent).

## Configure IP SLAs (TWAMP Responder)

The IETF Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip IP performance between any two devices that support the TWAMP protocols. The TWAMP-Control protocol is used to set up performance measurement sessions. It is used to send and receive performance-measurement probes. TWAMP enables complete IP performance measurement and provides a flexible choice of solutions as it supports all devices deployed in a network.

When you configure TWAMP using Cisco EPN Manager, the device you select is configured as a TWAMP server and you enter the TWAMP server configuration mode. It then uses the port value that you specify to configure the port to be used by the TWAMP server that listens for connection and control requests. The Inactivity Value that you specify will be configured as the inactivity timer (in seconds) for a TWAMP control session.



**Note** When you configure IP SLA using Cisco EPN Manager, the IP SLA responder is automatically configured on the device. You do not have to use the command *ip sla responder twamp* to pre-configure the IP SLA responder.

To configure interfaces for TWAMP:

### Before you begin

A TWAMP control-client and the session-sender must be pre-configured in your network before you can configure TWAMP responder using Cisco EPN Manager.

For IP SLAs TWAMP Responder v1.0, ensure that the TWAMP server and the session-reflector are configured on the same Cisco device.

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **IP SLA > TWAMP Responder** to add or edit the TWAMP Responder configuration.
- Step 5** Click the '+' icon to add the TWAMP parameters to the selected device. To edit existing parameters, click the Port Name hyperlink and click the Edit icon at the top right corner of the page. You can only add one set of TWAMP parameters per device.
- Step 6** Make your modifications to the following parameters. All parameters are mandatory.
- **Port-** Use a numeric value between 1 and 65535 to specify the port that must be configured for the TWAMP server to listen for connection and control requests. The default value is 862.
  - **Inactivity Timeout-** Use a numeric value between 1 and 604800 to specify the time that must be configured as the inactivity time (in seconds) for a TWAMP responder test session. The default value is 900 seconds.
  - **Server Inactivity Timeout-** Use a numeric value between 1 and 6000 to specify the time that must be configured as the TWAMP server inactivity time (in seconds) for a TWAMP control session. The default value is 900 seconds.
- Step 7** Click **Save** to deploy your changes to the device.
- If the deploy fails, ensure that the device's Inventory Collection status is 'Completed'. You also need to ensure that the pre-requisites mentioned above are met.
- 

## Configure Interfaces

Using Cisco EPN Manager , you can configure your CE and Optical Interfaces using the following configuration options:

Before you configure the interfaces, ensure that the device's Inventory Collection status is 'Completed'.

- [Configure Ethernet Interfaces and Subinterfaces, on page 295](#)
- [Configure Loopback Interfaces, on page 296](#)
- [Configure Tunnel Interfaces, on page 297](#)
- [Configure SwitchPort Interfaces, on page 298](#)
- [Configure Virtual Template Interfaces, on page 298](#)
- [Configure VLAN Interfaces, on page 299](#)
- [Configure Optical Interfaces, on page 300](#)
  - [Change the Loopback Settings on an Optical Interface, on page 300](#)
  - [Configure PRBS on ODU Controllers, on page 303](#)
  - [Continuous Verification of the Connection Status, on page 301](#)
  - [Enable and Disable OSC, on page 304](#)

- [Provision Optical Interfaces](#) , on page 305
  - [Change the Admin Status of an Optical Interface](#), on page 311
  - [Configure Protection Profiles](#), on page 312
  - [Configure TCM and TTI Parameters](#), on page 313
  - [Change the Payload and Breakout Settings](#), on page 315
  - [Configure OTN Interfaces](#), on page 316
  - [Enable and Disable GCC Connections](#), on page 317
  - [Configure Squelch Mode](#), on page 317
- [Example: Change the Admin Status for Cisco NCS 2006 Interface](#), on page 318

## Configure Ethernet Interfaces and Subinterfaces

The Configuration tab on the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can create, edit, delete, enable, and disable these interfaces.

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.

**Step 4** Choose **Interfaces > Ethernet**.

**Step 5** To add an Ethernet subinterface:

- a) Choose an Ethernet interface and click **Add Subinterface**.

**Note** This button is enabled depending on the device that you select. For example, on Cisco ASR903 devices, this button is disabled.

- a) In the Basic Configuration area, at a minimum, enter the **Interface Number** (if not already populated) and optionally provide a description for the subinterface.
- b) In the **VLAN Number** field, enter a numerical value that can be used to represent the VLAN ID for this subinterface. Note that only the 802.1Q type of encapsulation is supported.
- c) To use the same VLAN number as the native VLAN ID, enable the **Native VLAN** checkbox.
- d) In the **Dataplane Loopback** drop-down menu, select the value that must be set as the loopback value. Your options are: **Blank** (makes no change in the configuration), **None** (removes the Ethernet loopback from the interface), **Internal**, and **External**. The value that is already configured on the device is highlighted in the bold font.
- e) If you are creating an IPv4 subinterface, in the IPv4 Interface area, select an **IP Type**. Your options are:
  - None
  - Static IP, with the IP address and subnet mask.
  - DHCP IP, with the pool name.
  - DHCP Negotiated, with the hostname and client ID (None, Interface, Port Channel).

You can also enter a secondary IP address with mask.

- f) If you are adding an IPv6 subinterface, in the IPv6 Address area, select a type from the **Add** drop-down list. Your options are: Global, Unnumbered, Link Local, Auto Configuration, and DHCP.
- Global, with the IP address and subnet mask, and type (General, EUI-64, Anycast, CGA).
  - Unnumbered, and enter text in the Interface Unnumbered To text box.
  - Link Local, auto-configured or manually-configured (requires IPv6 address).
  - Autoconfiguration.
  - DHCP (with option to enable two-message exchange for address allocation).

If you choose to edit an existing interface or subinterface, you are allowed to change all values except the Interface Number value.

- g) Click **Save** to add the sub-interface to the selected interface of the device.

**Step 6** To enable, disable, or delete interfaces and subinterfaces, select the interfaces and click the appropriate buttons. The Delete Subinterface button may only be enabled on some supported devices, such as, Cisco ASR903 devices.

**Step 7** Click **Save** to deploy your changes to the device.

## Configure Loopback Interfaces

You can change the loopback state of an interface to test how your optical network is performing. Before changing the loopback setting, ensure that the device is either in Managed state or ideally in Complete state.

To change the loopback settings on an interface:

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.

**Step 4** Choose **Interfaces > Loopback**.

**Step 5** To specify a new loopback interface, click **Add**.

- a) In the Basic Configuration tab, specify the **Loopback Interface Number** (if not pre-populated).
- b) If you are creating an IPv4 loopback interface, specify an **IP Type**:
  - None.
  - Static: along with the IP address and subnet mask of the static IP address.
  - DHCP IP: along with the DHCP pool name.

You can also enter a secondary IP address with its mask so that it can be used as the backup loopback interface.

- c) If you are adding an IPv6 loopback interface, in the IPv6 Address area, select a type from the Add drop-down list. Your options are:
- Global- which also requires you to specify the IP address, subnet mask, and type (General, EUI-64, Anycast, CGA).
  - Unnumbered- which requires you to enter text in the Interface Unnumbered To text box.

- Link Local- which is either auto-configured or manually-configured and only applies to requires IPv6 address.
- Autoconfiguration
- DHCP- which also allows you to set the option to enable two-message exchange for automatic address allocation.

- Step 6** To edit an existing loopback interface, select the interface and click the **Edit** button to change only the speed, duplex, and other settings. The Interface Number cannot be edited.
- Step 7** To enable the above loopback settings on the interfaces, select the required loopback process and click **Enable**.
- Step 8** Click **Save** to deploy these configuration changes on the device.

## Configure Tunnel Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can create, edit, delete, enable, and disable these interfaces.

- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **Interfaces > Tunnel**.
- Step 5** To create a new tunnel interface, click **Add**.
- In the Basic Configuration area:
    - At a minimum, enter the Interface Number (if not already populated) and select a mode from the Tunnel Mode drop-down list.
    - (Optional) Enter a description, MTU (in bytes), bandwidth (in Kbps), Keepalive (in seconds) and number of keepalive retries. To avoid fragmentation, check the check box under MTU.
  - If you are creating an IPv4 tunnel interface, select an IP Type:
    - Static, with the IP address and subnet mask
    - DHCP IP, with the pool name

You can also enter a secondary IP address with mask.
  - If you are adding an IPv6 tunnel interface, in the IPv6 Address area, select a type from the Add drop-down list: Global, Unnumbered, Link Local, Auto Configuration, or DHCP.
    - Global, with the IP address and subnet mask, and type (General, EUI-64, Anycast, CGA)
    - Unnumbered, and enter text in the Interface Unnumbered To text box
    - Link Local, auto-configured or manually-configured (requires IPv6 address)
    - Autoconfiguration
    - DHCP (with option to enable two-message exchange for address allocation)
  - Optionally configure the tunnel source in the Advanced Configuration area by choosing Interface or IP address (with tunnel source interface, tunnel destination, and IPSec Profile).
- Step 6** To edit an existing tunnel interface, you can change the speed, duplex setting, and other parameters listed in the previous step except the Interface Number parameter.
- Step 7** To enable, disable, or delete a tunnel interface, select the interfaces and click the appropriate buttons.

**Step 8** Click **Save**.

---

## Configure SwitchPort Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can create, edit, delete, enable, and disable these interfaces.

---

- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **Interfaces > SwitchPort**.
- Step 5** To edit an interface, select the interface and click **Edit**.
- Choose and Administrative Mode: Static, Trunk 802.1Q, or Routed.
  - Enable or disable the port fast setting, and adjust the speed and duplex, if needed.
- Step 6** Click **Save**.
- 

## Configure Virtual Template Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can create, edit, delete, enable, and disable these interfaces.

---

- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **Interfaces > Virtual Template**.
- Step 5** To create a new virtual template interface, click **Add**.
- In the Basic Configuration area, at a minimum, enter the Interface Number (if not already populated), Type. Type can be Serial (with PPP, Slip, or FrameRelay encapsulation), Ethernet, or Tunnel (with tunnel mode).
  - If you are creating an IPv4 virtual template interface, select an IP Type:
    - Static, with the IP address and subnet mask
    - DHCP IP, with the pool nameYou can also enter a secondary IP address with mask.
  - If you are adding an IPv6 virtual template interface, in the IPv6 Address area, select a type from the Add drop-down list: Global, Unnumbered, Link Local, Auto Configuration, or DHCP.
    - Global, with the IP address and subnet mask, and type (General, EUI-64, Anycast, CGA)
    - Unnumbered, and enter text in the Interface Unnumbered To text box



- Link Local, auto-configured or manually-configured (requires IPv6 address)
  - Autoconfiguration
  - DHCP (with option to enable two-message exchange for address allocation)
- d) Optionally perform the advanced configurations:
- For Serial, the advanced configuration depends on the encapsulation type. For example, for Frame Relay, enter the LMI type (cisco, ansi, autosense, or q933a), and DLI. You can optionally choose to IETF encapsulation when connecting to non-Cisco routers.) For PPP, enter the authentication type (CHAP, PAP, both, with credentials).
  - Unnumbered, and enter text in the Interface Unnumbered To text box
  - Link Local, auto-configured or manually-configured (requires IPv6 address)
  - Autoconfiguration
- e) Specify the tunnel source in the Advanced Configuration area by choosing Interface or IP address (with tunnel source interface, tunnel destination, and IPsec Profile).
- Step 6** To edit an existing tunnel interface, you can change the speed, duplex setting, and other parameters listed in the previous step except the Interface Number parameter.
- Step 7** To enable, disable, or delete a tunnel interface, select the interfaces and click the appropriate buttons.
- Step 8** Click **Save**.

## Configure VLAN Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can create, edit, delete, enable, and disable these interfaces.

- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **Interfaces > Vlan**.
- Step 5** To add a VLAN interface, click **Add**.
- a) In the Basic Configuration area, at a minimum, enter the Interface Number (if not already populated). You can also enter a description, MTU (in bytes), and bandwidth (in Kbps).
  - b) If you are creating an IPv4 VLAN interface, select an IP Type:
    - Static, with the IP address and subnet mask
    - DHCP IP, with the pool name

You can also enter a secondary IP address with mask.
  - c) If you are adding an IPv6 VLAN interface, in the IPv6 Address area, select a type from the Add drop-down list: Global, Unnumbered, Link Local, Auto Configuration, or DHCP.
    - Global, with the IP address and subnet mask, and type (General, EUI-64, Anycast, CGA)
    - Unnumbered, and enter text in the Interface Unnumbered To text box
    - Link Local, auto-configured or manually-configured (requires IPv6 address)
    - Autoconfiguration

- DHCP (with option to enable two-message exchange for address allocation)

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

---

## Configure Optical Interfaces

Using EPN Manager you can configure your optical interfaces to change their admin settings, enable standard FEC modes on them, modify their payload settings, and change their loopback settings. To do this, use the Configuration tab in the Device Details page which lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can create, edit, delete, enable, and disable these interfaces.

You can configure optical interfaces in the following ways:

- [Change the Loopback Settings on an Optical Interface, on page 300](#)
- [Configure PRBS on ODU Controllers, on page 303](#)
- [Continuous Verification of the Connection Status, on page 301](#)
- [Enable and Disable OSC, on page 304](#)
- [View and Acknowledge Unverified Alarms, on page 305](#)
- [Provision Optical Interfaces , on page 305](#)
  - [Change the Admin Status of an Optical Interface, on page 311](#)
  - [Configure Protection Profiles, on page 312](#)
  - [Configure TCM and TTI Parameters, on page 313](#)
  - [Change the Payload and Breakout Settings, on page 315](#)
  - [Configure OTN Interfaces, on page 316](#)
  - [Enable and Disable GCC Connections, on page 317](#)
  - [Configure Squelch Mode, on page 317](#)
- [Example: Change the Admin Status for Cisco NCS 2006 Interface, on page 318](#)

### Change the Loopback Settings on an Optical Interface

You can change the loopback state of an interface to test how your optical network is performing. Before changing the loopback setting, ensure that the device is either in Managed state or ideally in Complete state. The interface that you want to modify must be in Maintenance (OOS, MT) admin state. EPN Manager allows you to edit the loopback settings only on SONET, SDH, Ethernet, FC/FICON, and OTN interface types.

To change the loopback settings on an interface:

---

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

- Step 3** Click the **Configuration** tab.  
For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.
- Step 4** Choose **Optical Interfaces > Maintenance > Loopback**.  
The interfaces of the selected device are displayed along with their loopback settings. Interfaces that are not supported, for example, Data Storage, OTS, or Video, are not displayed.
- Step 5** To edit the loopback settings, select the interface name (hyperlink) and click **Edit** to make your changes. Ensure that the device is in Managed or Complete state and the interface is in Maintenance (OOS, MT) admin state.
- a) Internal—this applies the same configuration applied in Terminal loopback.
  - b) Line—this applies the same configuration applied in Facility loopback.
  - c) No\_Loopback—Select this option to set no loopback values on the interface.
- Before you change the loopback state ensure that you first clear the current loopback setting using the No\_loopback option from the drop-down menu and then re-apply the setting of your choice.
- Step 6** Click **Save** to save your edits.  
A pop-up notification notifies you about the status of your changes.
- Note** If the Edit task fails, check if the device is in Managed or Completed state and ensure that Cisco EPN Manager is in sync with the device configuration. If not, resync the device with Cisco EPN Manager . See, [Collect a Device's Inventory Now \(Sync\)](#), on page 269.

## Continuous Verification of the Connection Status

Using the Connection Verification feature, you can view the power levels of optical interfaces and verify the interfaces for connectivity and insertion loss. Verifying the connectivity indicates whether the cable is in a connected state and verifying the insertion loss indicates whether the cable loss is within an expected value. The parameters for insertion losses are collected for every possible optical path inside the network element in order to predict possible failures.

Using Cisco EPN Manager you can view the Connection Verification parameters and opt to enable or disable Connection Verification on interfaces. You can also set the acknowledgment values for associated alarms.

To verify the connection status for your optical interfaces:

- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab.  
For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.
- Step 4** To enable or disable the Connection Verification feature and set the common threshold vales, click **Optical Interfaces > Provisioning > Connection Verification**.
- Step 5** Click the Edit icon at the top right corner of the page to edit common parameters.
- Step 6** Enter the following threshold parameters for the selected device and click **Save**:
- Connection Verification Enabled- Set to True or False to enable or disable this feature on the selected device.

- Fail IL Threshold (dB)- Enter a numerical value ranging from 0 to 20. When this threshold value is exceeded, an alarm is generated.
- Degree IL Threshold (dB)- Enter a value lesser than the failed IL threshold value.

**Step 7** Click **Optical Interfaces > Maintenance > Connection Verification Entry**.

For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.

**Step 8** Click the A Side hyperlink to view the following values of the connection:

- A Side- Displays the originating slot for connection verification.
- Z Side- Displays the destination slot for connection verification.
- Last Refresh- Displays the date and time when the connection verification and insertion loss verification was run previously.
- Connectivity Last Change- Displays the date and time when the connectivity information was previously changed.
- Connectivity Verification- Displays the status of connectivity:
  - Connected- Cable or patch cord is connected.
  - Disconnected- Cable or patch cord is disconnected.
  - Disabled- Cable or patch cord is excluded from connection verification.
  - Not Measurable- Power source not detected; cable or patch cord cannot be tested for connection verification.
  - Not Verified- Cable or patch cord is yet to be tested for connection verification.
- Excess Insertion Loss (dB)- Display the excess insertion loss that is higher than the set threshold.
- Insertion Loss Last Change- Displays the date and time when the insertion loss verification information was previously changed.
- Display names for- A and Z Side, A and Z Side Modules- identification names of the connection for A and Z Side, and A and Z Side Modules.

**Step 9** In the **Connection Verification Action** drop-down menu, choose an action that must be taken when the configured threshold values are reached, and click **Save**. Your options are: **Verify loss and connectivity**, **Disable verification**, and **Acknowledge loss alarm**.

**Step 10** (Optional) Select one of the following values to specify how alarms must be generated with respect to the Connection Verification parameters:

- **Acknowledge Loss Alarm** - allows the interfaces to operate beyond the Fail IL Threshold thresholds without raising an alarm. If the Fail IL Threshold further increases, alarms are raised again.
  - **Clear Acknowledge** - indicates that the Fail IL Threshold thresholds are set to default and alarms are re-evaluated. If thresholds are exceeded, an alarm is raised.
-

## Configure PRBS on ODU Controllers

Pseudo Random Binary Sequence (PRBS) is a testing mechanism used to ensure that the selected overhead bytes can be used to transport the header and trailer data safely. Both the transmitting node and receiving node must be aware that PRBS testing is taking place. To do this you can use Cisco EPN Manager to enable appropriate PRBS modes on the nodes. Cisco EPN Manager allows you to configure PRBS only on the non-channelized ODU controllers of an optical device.

PRBS also enables trunk ports to generate the PRBS\_31 pattern and detect PRBS\_11, PRBS\_23, and PRBS\_31 patterns.

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab.

For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.

**Step 4** Choose **Optical Interfaces > Maintenance > PRBS Configuration**. All ODU controllers and their current PRBS parameters are displayed. If the controllers are not listed, ensure that the above stated pre-requisites are met.

**Step 5** To configure PRBS, click the controller's name hyperlink and click the Edit icon at the top right corner of the page.

**Step 6** Make your modifications to the following parameters.

- a) In the **Admin State** drop-down list, select a valid admin state for the ODU controller. Your options are **00S-MT** (maintenance), **OOS-DSBLD** (disabled), and **IS** (inservice).

The PRBS parameters can be edited only if you set the Admin State to 00S-MT (maintenance) state.

To edit only the admin state of the controller, set the PRBS mode to Disabled, and choose the admin state of your choice.

- b) Select the PRBS Test value as **Enabled** or **Disabled**.
- c) Select the PRBS mode for the controller. When you set one controller with the values in column one (see below), ensure that the second controller (node 2) is set with the corresponding values shown in the second column of this table:

Controller 1 Mode (Node 1)	Controller 2 Mode (Node 2)
Source	Sink
Sink	Source
Source-Sink	Loopback
Loopback	Source-Sink

- d) From the **Pattern** drop-down list, select one of the following PRBS patterns. This pattern will be either generated or detected by the line cards:
  - NONE
  - PN11
  - PN23
  - PN31

- INVERTEDPN11
- INVERTEDPN31

**Step 7** Click **Save** to deploy the updated configuration to the device.

**Step 8** (Optional) To verify, view updated PRBS parameters in the **Configuration** tab for the selected controller, under **Optical Interfaces > Provisioning > PRBS**. To run a PRBS test on ODU UNI circuits, see, [Run PRBS Test on Circuits \(ODU UNI\)](#), on page 563.

## Enable and Disable OSC

Using Cisco EPN Manager, you enable or disable the Optical Service Channel (OSC) terminations on the interfaces of optical devices. OSC can be configured on OC3 lines, and on FastEthernet (FSTE) and GigabitEthernet (GigE) interfaces of the following cards:

- Transmission Network Control System (TNCS)
- Transport Node Controller - Enhanced (TNCE)
- Transport Node Controller (TNC)

For ONS15454 NEs, the supported interfaces are OC3 interfaces of the following cards:

- Optical Service Channel Modem (OSCM)
- Optical Service Channel and Combiner/Separator Module (OSC-CSM)

To configure OSC on optical devices:

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab.

For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.

**Step 4** Choose **Optical Interfaces > Comm Channels**.

All configurable G709 enabled interfaces of the selected device are displayed.

**Step 5** Click the **OSC** tab.

**Step 6** Choose the communication channel that you want to configure by clicking the communication channel's name hyperlink.

The communication channel name and current OSC setting is displayed.

**Step 7** Click the Edit icon at the top right of the page.

**Step 8** Use the **OSC** checkbox to enable or disable OSC on the selected communication channel.

**Step 9** Click **Save**.

Your changes are saved and the updated configuration is deployed to the device. To verify, view the OSC settings for the selected communication channel under **Optical Interfaces > Provisioning > Comm Channels**.

## View and Acknowledge Unverified Alarms

Based on the alarm generated on your devices, you can view the details of the alarm in Unverified status and then mark them Acknowledged so that they no longer appear as unread alarm notifications on the device. To do this:

- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab.  
For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.
- Step 4** Choose **Optical Interfaces > Maintenance > Unverified Alarms** to view the alarms with the Unverified status.
- Step 5** Once you have reviewed the alarms and taken the required action, select the alarms and click the **Acknowledge** button to mark these alarms Verified directly on the device.

## Provision Optical Interfaces

You can use Cisco EPN Manager to enable the following configuration options on your optical devices.



**Note** The following configuration options are enabled or disabled depending on the device you select. To check whether your device supports these options, see [Supported Devices for Cisco EPN Manager](#).

### • Ethernet MTU

Using Cisco EPN Manager you can configure the MTU values on the Ethernet interfaces of your optical devices. The MTU is the Maximum Transmission Size, in bytes, of a packet passing through the interface. You can use Cisco EPN Manager to modify the MTU values on all Ethernet interfaces except Gigabit Ethernet and Fast Ethernet interfaces on TNC and ECU modules.

To verify that your new Ethernet MTU values are configured on the device, navigate to your device's Device Details page and click the Ethernet Interface tab.

### • GMPLS

Using Generalized Multi-Protocol Label Switching (GMPLS), you can define and view the fiber and alien wavelength parameters that are used during GMPLS circuit creation. It ranges the packet based data on the MPLS protocol to allow the creation and maintenance of channels across the networks. It supports non-packet switching devices. This means that GMPLS extends the packet based MPLS protocol to allow creation and maintenance of tunnels across networks that consist of non-packet switching devices. GMPLS tunnels can traverse Time-Division Multiplex (TDM) interfaces and switching types.

To configure GMPLS, you can use the Configuration tab in Cisco EPN Manager which allows you to configure GMPLS on all LMP enabled optical controllers. The enabling of LMP which is a pre-requisite for GMPLS configuration can also be done using the same Configuration tab.



---

**Note** You cannot disable GMPLS on LMP enabled controllers that are part of active optical circuits.

---

#### • Packet Termination

Using Cisco EPN Manager you can set up packet termination on the ODU controllers of your optical devices. To do this, ensure that packet termination is pre-configured on the device for Ethernet packets. You can then edit the configuration that is already created on the device and discovered by Cisco EPN Manager.

To configure packet termination, you must specify both the Termination Mode and Mapping Mode values.

#### • LMP

The Link Management Protocol (LMP) helps in managing channels and links that are required between nodes for routing, signaling, and link management. LMP is also used to manage the Traffic Engineering (TE) link. It allows multiple data links into a single Traffic Engineering (TE) link that runs between a pair of nodes.

To create an LMP neighbor using Cisco EPN Manager, you need to specify the neighbor's name, link ID, router ID, and interface ID, and the common link and interface IDs. You can add only one LMP link per controller on your optical device.

While the LMP configuration can be successfully deployed to a single device using Cisco EPN Manager, for LMP to function effectively, you need to configure it on both sets of devices that are participating in the link. This ensures that the LMP link is activated.

Limitations:

- Although LMP is supported on Cisco NCS 40XX and Cisco NCS 20XX devices individually, LMP links cannot be created between Cisco NCS 20XX and Cisco CRS devices.
- You cannot edit the Numbering value of an LMP link after it has been created. To edit the Numbering value, delete the LMP link and recreate it with the new Numbering value.
- You cannot have duplicate Neighbor Router IDs between two LMP neighbors.
- When you add an LMP link, ensure that the controller is not already associated with another LMP link. This will cause your deploy to fail.

#### • OTN Topology

You can use the Configuration tab to add or modify the topology instance and Area ID associated with an optical OTN controller. If the controller does not have a pre-configured Topology Instance and Area ID, Cisco EPN Manager automatically sets the topology instance to OTN and the Area ID to 0.

Cisco EPN Manager does not allow you to use the same topology instance and Area ID that is already pre-configured on other controllers. To know the Topology Instance and Area ID that is pre-configured on the device, go to **Maps > Network Topology**.

#### • NNI



You can configure your optical interfaces to act as network-node interfaces (NNIs). An NNI indicates that the interface connects to other network nodes. Cisco EPN Manager allows you to configure NNIs on the OTU controllers of your optical device. These interfaces can further be configured to act as source and destination ports.

If a device is not part of a topology, configuring its NNI controller creates an OTN topology instance for that controller with an Area ID 0.

You can create only one NNI configuration per controller for every controller present on the device.

Note: You cannot delete NNI controllers that are pre-configured with a Topology Instance.

#### • Breakout

Enabling breakout on your optical devices utilizes the multilane architecture of the optics and cables to enable you to split single higher density ports into multiple lower density ports. For example, a 100G port can be configured to operate as ten different 10G ports. Or a single 40G port can act as four different 10G ports. To configure breakout using Cisco EPN Manager, see the table below.

Pre-requisite:

Ensure that Breakout is pre-configured on the interface by changing the interface's Port Mode value to Breakout. See [Change the Payload and Breakout Settings, on page 315](#). This changes all other port mode parameters of that interface to 'None' enabling breakout on the port, thus allowing you to configure lanes. You can add up to ten lanes per interface.

Limitations:

- All lanes that belong to a particular interface must have the same mapping type.
- OTU2 and OTU2e controllers are supported only if they are in the packet termination mode.
- In Cisco NCS 5.2.4x devices, breakout lanes can only be created when the port modes are of type Ethernet.
- 10G clients that are mapped to OPU2e framing type are not supported.
- Breakout cannot be configured on SONET and SDH controllers.

Example configuration:

If you select a controller optics 0/0/0/0 and enable Breakout with GFPF as its mapping mode and with a framing value of OPU2, then the configuration pushed to the device is:

```
controller optics 0/0/0/0 breakout-mode 1 ethernet framing opu2 mapping gFpF
```

#### • Performance Monitoring

Performance Monitoring (PM) helps you gather performance counters for system maintenance and troubleshooting. You can retrieve both current and historical PM counters at regular intervals. You can enable and disable performance monitoring on OTU and ODU controllers of an optical device.

To configure performance monitoring at the TCM controller level, you must configure OTN interfaces and their associated TCM performance counters, see:

- [Reference—Performance Counters for OTN-FEC Interfaces, on page 775](#)
- [Reference—Performance Counters for OTN-ODU Interfaces, on page 775](#)
- [Reference—Performance Counters for OTN-OTU Interfaces, on page 776](#)

**• Channelize ODU (LO) Controllers:**

Associate your ODU controllers with multiple lower order ODU sub-controllers and configure tributary port number (TPN) and tributary slots (TS) for those ODU sub-controllers. A valid range of TPN is from 1 to 80. If a TS string is separated using a colon (:), this indicates individual tributary slot. If a TS string is separated using an en-dash (-), this indicates a range of tributary slots.

When you select the ODU level for the sub-controllers, ensure that the sub-controller's ODU level is lower than that of the main controller you are associating it with. For example, if you are associating sub-controllers with an ODU controller of ODU3 level, then the sub-controllers can be of levels ODU2, ODU1, or ODU0.

**• Configuring OTDR Settings:**

Using this feature, you can configure OTDR scans to begin automatically on a fiber span that has been repaired or on the startup of an OSC channel. To do this, ensure that the 'Auto Scan on LOS' parameter is enabled. A fiber is considered to be repaired when the LOS on the fiber is cleared and an alarm is raised based on the following criteria:

- If you check the Enable Absolute Threshold checkbox, the 'OTDR-LOSS-THR-EXCEEDED' alarm is raised when the insertion loss measured for the OTDR scan is greater than the Absolute Event Loss Threshold (dB) value configured.
- If the total back reflection for the OTDR scan is less than the Total Back Reflection (dB) value that you specify.
- If the Absolute Pass Fail Criteria is disabled, the Loss and Back Reflection values from the baseline scan in the previous release are considered as threshold values. In this scenario, the OTDR-LOSS-THR-EXCEEDED alarm is raised.

Depending on how you want the auto scans to be triggered, you can configure the following parameters:

- Auto Scan on Span Loss Increase- OTDR scan starts automatically on the fiber if the measured span loss on the fiber is greater than the threshold value configured. The default threshold value is 2.
- Enable OLR continuous measurement on Rx direction- measures the span loss in the LINE-RX port (input) of the card depending on the configured threshold value.
- Enable WDM Side from WSON Provisioning- prevents creation of circuits when the Loss and Back reflection threshold values are crossed during an OTDR scan.

You can configure the Event Loss Threshold value within which the total span loss on the fiber is permitted. If the measured span loss on the fiber is greater than the Event Loss Threshold value, then the OTDR scan is triggered on the fiber.

**• Configure Automatic Laser Shutdown (ALS):**

Automatic Laser Shutdown (ALS) is a technique used to automatically shut down the output power of the transmitter in case of issues such as a fiber break. This is a safety feature that prevents dangerous levels of laser light from leaking out of a broken fiber, provided ALS is provisioned on both ends of the fiber pair. Once an interface has been shut down, you can configure the action that must be taken to restart the interface by setting the ALS mode to:

- **Disabled mode**—If mode is disabled, ALS is disabled. Loss Of Signal (LOS) will not cause laser shutdown.

- **Manual restart mode**—The laser is turned off when the ALS agent detects an LOS for 500 ms. After ALS is engaged, a manual command is issued that turns on the laser for the time period of the pulse width. The laser is turned on when the LOS has been cleared for 100 ms.
- **Automatic restart mode**—The laser is shut down for the time period of pulse spacing when the ALS agent detects a LOS for 500 ms. Then, the laser automatically turns on for the time period of the selected pulse width. If an LOS still exists at that time, the laser is shut down again. This pattern continues until the LOS is cleared for 100 ms; then, the laser will stay on.

Cisco EPN Manager enables you to set the ALS mode, the ALS recovery interval (in seconds), and the recovery pulse width (in seconds). If the ALS Mode for the interface has been set to Manual Restart, you need to manually restart the interface. To do this, navigate to the device's Device Details page, choose **Optical > Automatic Laser Shutdown**, locate the interface set to the Manual Restart ALS mode, and click the **Restart** button.

- **Using the SNTP Server to Set the Date and Time:**

Simple Network Time Protocol (SNTP) is an internet protocol used to synchronize the clocks of computers to a time reference. Using the SNTP server ensures that all NEs use the same date and time reference. The server synchronizes the node's time after power outages or software upgrades.

To use the SNTP server to set the date and time you must first specify the current time along with the time zone value and then set the primary and backup servers that can be used as a point of reference for the date and time. Before you set the timezone values, ensure that the SNTP server values are not configured. When you delete an SNTP server, ensure that you first delete the Backup server and only then the Primary server. You cannot delete only the Primary server.

- **Configuring the Wavelength:**

Cisco EPN Manager enables you to provision the wavelength frequency for your optics controllers. You can view the current wavelengths configured on the optics controllers and then depending on the type of card selected, you can change the wavelength frequency.

You can configure the wavelengths on an optics controller only when it is configured as a DWDM optics port. To confirm this, navigate to the device's Device Details page, choose **Interfaces > Optical Interfaces**, and check if the Optics Type column for the interface is either **DWDM** or **Grey**.

### Table- Provisioning Optical Interfaces

To configure your optical devices with the above features:

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab.  
For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.
- Step 4** Navigate to the required configuration menu as described in the table below, and specify the required values.

**Table 18: Table- Configuring Optical Interfaces**

Task	Supported Interfaces/Controllers	Navigation	Notes
------	----------------------------------	------------	-------

Configuring Ethernet MTU	All Ethernet interfaces except Gigabit/Fast Ethernet interfaces on TNC and ECU modules.	Optical Interfaces > Provisioning > Ethernet MTU	-
Configuring GMPLS	LMP enabled optical controllers.	Optical Interfaces > Provisioning > GMPLS	-
Configuring Packet Termination	ODU controllers pre-configured with Packet Termination.	Optical Interfaces > Provisioning > OTN > Packet Termination	Applicable only to Ethernet packets.
Configuring an LMP Neighbor	All optical controllers.	Optical Interfaces > Provisioning > LMP	Neighbor Router ID cannot be duplicated between neighbors
Configuring OTN Topology	All optical OTN controllers.	Optical Interfaces > Provisioning > OTN > Topology	-
Configuring NNI	All OTU controllers.	Optical Interfaces > Provisioning > OTN > NNI	-
Configuring Breakout	All optical controllers with Port Mode values set to 'Breakout'.	Optical Interfaces > Provisioning > Port Mode > Breakout tab	-
Configuring Performance Monitoring	All OTU and ODU controllers.	Optical Interfaces > Provisioning > Performance Monitoring	-
Channelize ODU (LO) Controllers	All ODU controllers.	Optical Interfaces > Provisioning > ODU Channelization > Sub-Controllers tab	-
Configuring OTDR Settings	-	Optical Interfaces > Provisioning > OTDR Settings	-
Configuring ALS	All ALS supported interfaces	Optical Interfaces > Provisioning > Automatic Laser Shutdown	-

Setting the Date and Time using SNTP	-	<ul style="list-style-type: none"> <li>To specify the primary and backup servers for SNTP: Choose Optical Interfaces &gt; Provisioning &gt; NTP Settings</li> <li>To specify the current time and time zone that can be used by SNTP: Choose Optical Interfaces &gt; Provisioning &gt; Time Zone Settings</li> </ul>	-
Configure Wavelength	All optics controllers	Optical Interfaces > Provisioning > Wavelength	-
Configure TCM and TTI	-	See <a href="#">Configure TCM and TTI Parameters, on page 313</a>	-
Configure Protection Profiles	-	See <a href="#">Configure Protection Profiles, on page 312</a>	-
Configure the Payload and Breakout Settings	-	See <a href="#">Change the Payload and Breakout Settings, on page 315</a>	-
Configure the Admin Status	-	See <a href="#">Change the Admin Status of an Optical Interface, on page 311</a>	-
Configure FEC Mode	-	See <a href="#">Configure OTN Interfaces, on page 316</a>	-
Enabling and Disabling GCC	-	See, <a href="#">Enable and Disable GCC Connections, on page 317</a>	-
Configure Squelch Mode	-	See, <a href="#">Configure Squelch Mode, on page 317</a>	-

## Change the Admin Status of an Optical Interface

Cisco EPN Manager enables you to change the admin state of an interface to enhance the performance testing abilities for your optical network. The Admin Status of an interface defines whether the interface is being managed by Cisco EPN Manager, whether it is down, or whether it is in maintenance mode. When the admin

status of an interface is down, it indicates that the interface is in an unreachable state, or that the device is not supported by Cisco EPN Manager . Changing the admin status to Up enables Cisco EPN Manager to manage the interface and thus provide better monitoring capabilities. To change the admin state on an interface:

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab.  
For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.
- Step 4** Choose **Optical Interfaces > Provisioning > Admin Status**.  
The interfaces of the selected device are displayed along with their Admin State settings. Interfaces on which you cannot modify the admin state, for example, PCHAN and PLINE interfaces are not displayed.
- Step 5** Click either the **Optical Controllers** or **Ethernet Controllers** tab to edit the required controllers.
- Step 6** To edit the admin status, select the interface by clicking the interface's Name hyperlink, and then click the **Edit** icon at the top right corner of the page. Ensure that the device's inventory collection status is in Managed or Completed state.  
Choose one of the following values:
- a) **Down**—implies that the interface will be administratively down.
  - b) **Up**—implies that the interface will be administratively up.
  - c) **Testing**—implies that the interface is in Maintenance state and that the administrator is performing tests using it.
- Step 7** Click **Save** to save to deploy your changes to the device.  
A pop-up notification notifies you about the status of your changes. To see an example of the admin status being changed on a Cisco NCS2K device, see [Example: Change the Admin Status for Cisco NCS 2006 Interface, on page 318](#).
- Note** If the Edit task fails, check if the device is in Managed or Completed state and ensure that Cisco EPN Manager is in sync with the device configuration. If not, re-sync the device with Cisco EPN Manager as described in [Collect a Device's Inventory Now \(Sync\), on page 269](#).
- 

## Configure Protection Profiles

Using Cisco EPN Manager , you can provision different protection profiles (or groups) for your optical devices. This ensures availability and improved reliability for these devices. Protection profiles define whether Automatic Protection Switching (APS) must be enabled on the cards and they also set the direction for traffic flow in case of failures. The cards on the device can either be set to support unidirectional regeneration of configuration or can be set to ensure that both transmit and receive channels will switch when a failure occurs on one.

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab.  
For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.
- Step 4** Choose **Optical Interfaces > Provisioning > Protection Profile**.
- Step 5** To add a protection profile, click the + symbol.

- Step 6** Provide a unique name for the protection profile. The name is a mandatory field and should not contain space or exceed 32 characters.
- Step 7** Select the required type for the protection profile. Your options are:
- **One plus one BDIR APS**- Enables one plus one Automatic Protection Switching (APS) and configures the card to be bidirectional.
  - **One plus one UNIDIR APS**- Enables one plus one APS and configures the card to be unidirectional.
  - **One plus one UNIDIR NO APS**- Enables one plus one with no APS and configures the card to be unidirectional.
  - **One plus one PLUS R BDIR APS** - Enables one plus one plus R APS and configures the card to be bidirectional.
- Note**
- BDIR (bidirectional) indicates that both transmit and the receive channels will switch if a failure occurs on one.
  - UNIDIR (unidirectional) indicates that the card supports unidirectional regeneration of configuration. Hence the ports can only be used as the link source if they are transmit ports and as the link destination if they are receive ports.
- Step 8** Select the protection mode for the profile as **Revertive** or **Non-Revertive**. Revertive mode ensures that the node returns traffic towards the working port post a failure condition after the amount of time specified as the Wait to Restore Time (step 9).
- Step 9** Select the sub network connection mode as **SNC\_N** (default), **SNC\_I**, or **SNC\_S**.
- Step 10** When you select the sub network connection mode as **SNC\_S**, you can then select TCM-ID value from the TCM drop-down list. By default, TCM-4 is selected once you select SNC\_S as Sub Network Connection mode. You can change the TCM-ID column value from TCM4 to TCM1-TCM6 for SNC\_S.
- Note** For SNC\_I and SNC\_N, you are not allowed to change the TCM-ID value. It should be set to **None**.
- Step 11** Enter a value for the Wait to Restore Time in seconds using a number between 0 and 720. For any value greater than 0, ensure that the value is greater than 300 and in intervals of 30 seconds. The wait to restore time defines the time the system must wait to restore a circuit. If you have selected the protection mode as Revertive, then the default wait to restore time is 300, else it is 0.
- Step 12** Enter a value for the **Hold Off Time** in milliseconds. This value defines the time the system waits before switching to the alternate path. The valid range is from 100 to 10000 seconds. Default value is 0.
- Step 13** Click **Save** to deploy the updated changes to your device.
- Step 14** (Optional) To verify, view the updated protection profile parameters in the **Configuration** tab for the selected controller, under **Optical Interfaces > Provisioning > Protection Profile**.

## Configure TCM and TTI Parameters

Using Cisco EPN Manager you can configure Tandem Connection Monitoring (TCM) and Trail Trace Identifiers (TTI) on ODU controllers of ODU Tunnel circuits. This helps you enable and disable performance monitoring capabilities on these controllers.

You can further monitor your device's capabilities by configuring the threshold for signal failure and signal degrading in the TCM connections of these ODU controllers. You can also modify the source and destination access point identifiers. To do this, ensure that the following pre-requisites are met.

**Before you begin**

- Ensure that the device's inventory collection status is 'Completed'.
- Ensure that the controllers are configured for Loopback. If not, change the controllers loopback settings under **Optical Interfaces > Maintenance > Loopback**. See [Configure Loopback Interfaces, on page 296](#).



**Note** For the endpoints of an ODU UNI circuit, TCM is supported only on OTUx-ODUx controllers.

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab.

For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.

**Step 4** To configure TCM/TTI parameters, choose **Optical Interfaces > Provisioning > TCM Configuration**.

Alternatively you can navigate to the device's Chassis View tab, select a card from the Chassis Explorer, click the **Configuration** tab, and choose **OTN > Trail Trace Identifier**.

**Step 5** To view or edit the TCM parameters of any of the listed controllers, click the TCM ID hyperlink of that controller.

**Step 6** To edit these parameters, click the Edit icon at the top right corner of the page.

**Step 7** Make your changes to the following TCM parameters:

Editable TCM Parameters	Descriptions
State	Configures the state of TCM properties on the device as enabled or disabled.
Signal Failure Threshold	Configures the threshold value for signal failures on ODUk controllers. The values are E6, E7, E8, and E9.
Sent API	Configures the source access point identifier of the TTI. Enter a value of up to 14 bytes in length.
Sent DAPI	Configures the destination access point identifier of the TTI. Enter a value of up to 14 bytes in length.
Sent Operator Specific String Type	Configures the type of the operator specific string of the TTI as hexadecimal or ASCII type.
Sent Operator Specific String	Configures the operator specific string of the TTI. Enter a value of up to 32 characters in length.
Performance Monitor	Enables or disables performance monitoring on an ODUk controller.
Signal Degrade Threshold	Configures the signal degrade threshold value. The values are: E6, E7, E8, and E9.
Expected SAPI	Configures the current source access point identifier of the TTI. Enter a value of up to 14 bytes in length.



Editable TCM Parameters	Descriptions
Expected DAPI	Configures the current destination access point identifier of the TTI. Enter a value of up to 14 bytes in length.
Expected Operator Specific String Type	Configures the type of the operator specific string of the TTI as hexadecimal or ASCII type.
Expected Operator Specific String	Configures the operator specific string of the TTI. Enter a value of up to 32 characters in length.

**Step 8** Click **Save** to deploy the updated configuration to the device.

**Step 9** (Optional) To verify, view the selected device's TCM parameters in the Configuration tab, under **Optical Interfaces > Provisioning > TCM Configuration**.

**Step 10** (Optional) You can view these updated TCM and TTI parameters in the Device Details and Port 360 view of the selected device. See [View Device Details, on page 63](#) and [View a Specific Device's Interfaces: Device 360 View, on page 83](#).

**Step 11** (Optional) The TCM parameters are also represented on the network topology overlay. To view these parameters, navigate to **Maps > Network Topology** and select an optical circuit with these associated TCM parameters.

## Change the Payload and Breakout Settings

Using the Device Configuration tab, you can view and modify the type of the payload for packets on SONET and SDH interfaces and enable breakout on them. Before changing the payload setting, ensure that the device is in sync with Cisco EPN Manager . Enabling breakout on your optical devices utilizes the multilane architecture of the optics and cables to enable you to split single higher density ports into multiple higher density ports. For example, a 100G port can be configured to operate as ten different 10G ports. Or a single 40G port can act as four different 10G ports.

To change the payload and breakout setting on an interface:

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab.

For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.

**Step 4** Choose **Optical Interfaces > Provisioning**.

**Step 5** Depending on the type of device that you have selected, choose **Payload Type** or **Port Mode**

**Step 6** Click the name (hyperlink) of the interface that you want to modify.

Common properties of the interface such as its name and its payload type are displayed.

**Step 7** Click the name (hyperlink) of the OTN interface that you want to modify and click the Edit icon.

**Step 8** Make your changes to the Port Mode, Framing, Mapping Type, Rate, and Bit Rate values. Ensure that these values do not exceed the card's bandwidth limitations.

**Step 9** To associate breakout lanes for Ethernet and OTN packets on this interface, click the **Breakout** tab. This tab is only displayed if the device has breakout pre-configured.

- a) Click the '+' icon to add a new lane. You can add up to 10 lanes per controller. To modify existing lanes, click the Lane hyperlink.
- b) Specify the breakout parameters such as the lane number, the port mode and mapping type for the breakout lane, the owning port number, and the framing value.

**Step 10** Click **Save** to deploy your changes to the device.

A pop-up notification notifies you about the status of your changes.

**Note** If the Edit task fails, check if the interface is in Managed state and ensure that Cisco EPN Manager is in sync with the device's configuration. If not, resync the device with Cisco EPN Manager. See [Save Your Device Changes, on page 269](#). You also need to ensure that the payload does not exceed the card's bandwidth limitation.

## Configure OTN Interfaces

The FEC Mode defines an OTN circuit's forward error correction (FEC) mechanism. The forward error correction (FEC) mechanism provides performance gains for improved margins and extended optical reach. To change the FEC Mode setting to Standard, you need to use the Device Configuration tab.

Before changing the FEC mode setting, ensure that the admin state of the interface you are trying to modify is in Down (out of service) state with G709 configuration enabled. To enable G709 configuration, use the OTN Lines configuration in the Chassis view.

To change the FEC mode on an interface:

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab.

For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.

**Step 4** Choose **Optical Interfaces > Provisioning**.

**Step 5** Change the admin state of OTN interfaces for which FEC needs to be modified to Down. See [Change the Admin Status of an Optical Interface, on page 311](#).

**Step 6** Depending on your device type, choose one of the following and select the interface you want to modify:

- **OTN Lines > OTNFEC**
- **OTN > FEC**

All configurable G709 enabled interfaces of the selected device are displayed.

Alternatively, you can navigate to the device's Chassis View tab, select a card from the Chassis Explorer, click the **Configuration** tab, and choose **OTN > OTN Lines**. This option enables you to configure additional parameters such as enabling the sync messages, choosing the admin SSM, enable the Provide Sync parameter, and set the G709 value to true or false.

**Step 7** Select the interface you want to edit, and click the Edit icon at the top right of the window.

**Step 8** Select the required FEC Mode. The default is None.

**Step 9** (Cisco NCS 2000 devices only) Select the required **SDBER** value. Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade alarm will occur for line degradation based on the threshold value that you set.

**Step 10** Click **Save** to save your changes.

A pop-up notification notifies you about the status of your changes.

**Note** If the Edit task fails, check if the interface is in Managed or Completed state and ensure that Cisco EPN Manager is in sync with the device's configuration. You also need to ensure that G709 configuration is enabled on the device. To change the admin state of the interface see, [Change the Admin Status of an Optical Interface, on page 311](#).

---

## Enable and Disable GCC Connections

Cisco EPN Manager supports the provisioning of Generic Communication Channel (GCC) connection on the interfaces of optical devices. GCC can be configured on trunk ports of TXP or MXP cards and on OTN, OTU, and ODU controllers. The GCC configuration can be modified irrespective of the FEC modes and admin statuses configured on the interfaces.

To configure GCC on optical devices:

---

**Step 1** Choose **Configuration > Network Devices**. All Cisco EPN Manager devices are displayed.

**Step 2** Select the optical device that you want to configure by clicking the device name hyperlink.

**Step 3** Click the **Configuration** tab and choose **Optical Interfaces > Provisioning**.

**Step 4** Depending on your device type, choose one of the following:

- **Comm Channels > GCC**
- **OTN > GCC**

All configurable G709 enabled interfaces of the selected device are displayed.

**Step 5** Click the **OTU Controllers** or **ODU Controllers** tab based on the type of controller that you want to edit.

**Step 6** To edit the GCC configuration of any of the listed controllers, click the controller's name hyperlink.

**Step 7** Click the Edit icon at the top right of the page.

**Step 8** Use the **GCC** check box to enable or disable GCC on the selected controller. The value configured on ODU controllers is GCC1 and that on OTU controllers is GCC0.

**Step 9** Click **Save**. Your changes are saved and the updated configuration is deployed to the device.

To verify, view the GCC parameters for the selected controller under **Optical Interfaces > Provisioning**.

---

## Configure Squelch Mode

Using Cisco EPN Manager, you can configure different squelch modes on the interfaces of optical devices. Squelch modes help shut down the far-end laser in response to certain defects. Squelch modes can be configured on OCH, OTN, SONET or SDH, FC or FICON, Ethernet, Video, and Data Storage interfaces of optical devices.

---

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

**Example: Change the Admin Status for Cisco NCS 2006 Interface**

- Step 3** Click the **Configuration** tab.  
For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Logical View tab that is at the top of the Device Details page.
- Step 4** Choose **Optical Interfaces > Provisioning > Squelch Mode**.
- Step 5** Choose the interface that you want to configure by clicking the interface's name hyperlink.  
The interface's name and current squelch mode setting are displayed.
- Step 6** Click the Edit icon at the top right corner of the page.
- Step 7** Select the required squelch mode for the interface. Your options are:
- **DISABLE**- Squelch is disabled.
  - **AIS**- Alarm Indication Signal (AIS) is enabled.
  - **NONE**- Transparent mode is enabled.
  - **SQUELCH**- Squelch is enabled.
  - **ODU\_AIS**
  - **G\_AIS**- Generis AIS is enabled.
  - **NOS**- Squelch is disabled in FC payloads.
  - **LF**
- Step 8** Click **Save**.  
Your changes are saved and the updated configuration is deployed to the device. To verify, view the squelch mode parameters of the selected interface under **Optical Interfaces > Squelch Mode**.
- 

**Example: Change the Admin Status for Cisco NCS 2006 Interface**

This example illustrates how to change the admin status for a Cisco NCS 2006 VLINE interface. In this example, the configuration change is launched from the Device Details page, but under the **Logical View** tab. (For other devices, configuration changes are performed under the **Configuration** tab.)

---

- Step 1** On the Device Details page under the Logical View tab, click the hyperlink for the interface you want to edit.

Home / ... / Device Management / Network Devices / Device Group / All Devices ★

Chassis View Logical View Device Details

**Features**

Search All

- Optical Interfaces
  - Maintenance
  - Provisioning
    - OTN Lines
      - Adminstatus**
      - Automatic Laser Shutdown
      - Comm Channels
      - Ethernet MTU
      - NTP Settings
      - OTDR Autoscan
      - Payload

**Admin Status**

Optical Controllers Ethernet Controllers

	Name	Display Name	Admin Status
	VLIN		
<input type="checkbox"/>	VLIN-5-7-1-1-10	VLIN-5-7-1-1-10	UP
<input type="checkbox"/>	VLIN-5-7-1-1-11	VLIN-5-7-1-1-11	UP
<input type="checkbox"/>	VLIN-5-7-1-1-2	VLIN-5-7-1-1-2	UP
<input type="checkbox"/>	VLIN-5-7-1-1-3	VLIN-5-7-1-1-3	UP
<input type="checkbox"/>	VLIN-5-7-1-1-6	VLIN-5-7-1-1-6	UP
<input type="checkbox"/>	VLIN-5-7-1-1-7	VLIN-5-7-1-1-7	UP

414925

**Step 2** In the interface's Common Properties window, click the Edit icon at the top right corner of the window.

Home / ... / Device Management / Network Devices / Device Group / All Devices ★

Chassis View Logical View Device Details

**Features**

Search All

- Optical Interfaces
  - Maintenance
  - Provisioning
    - OTN Lines
      - Adminstatus**
      - Automatic Laser Shutdown
      - Comm Channels

**VLIN-5-7-1-1-10**  
Admin Status

Common Properties

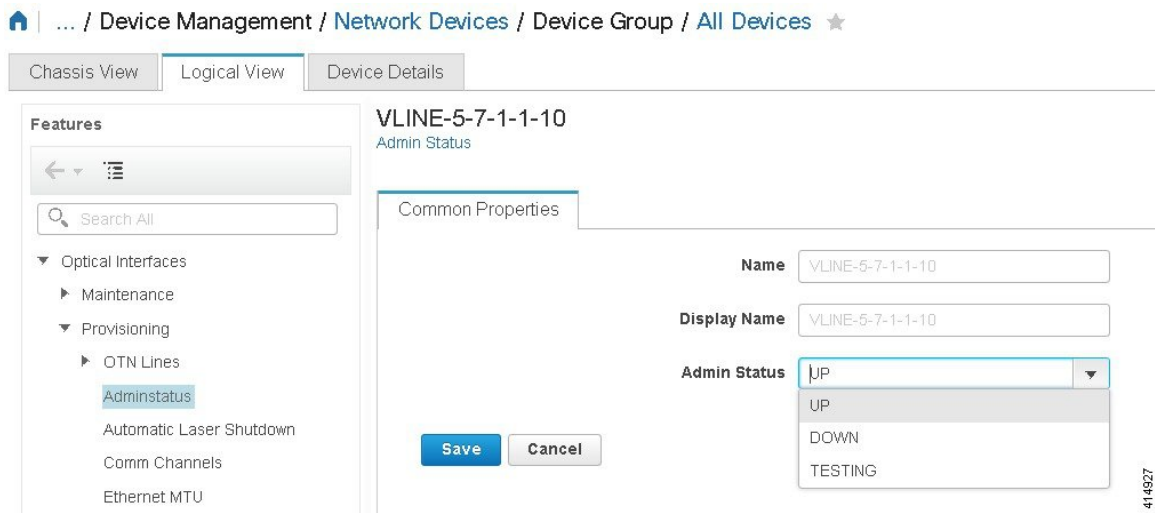
**Name** VLIN-5-7-1-1-10

**Display Name** VLIN-5-7-1-1-10

**Admin Status** UP

414926

**Step 3** Choose a new setting from the **Admin Status** drop-down list, then click **Save**.

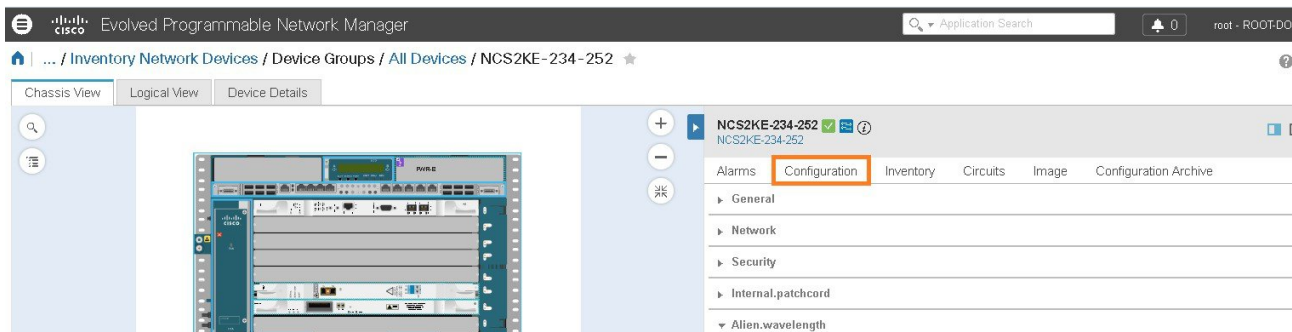


## Configure Devices Using the Chassis View

You can configure devices and cards from the devices' Chassis View. This can only be done from the **Configuration** sub-tab in the Chassis View. The sub-tabs are displayed depending on the type of device you select in the **Network Devices** page.



**Note** This feature is available only for Cisco NCS 2000 and Cisco ONS devices.



**Step 1** From the left sidebar, choose **Configuration > Network Devices**.

**Step 2** Select the device that you want to configure by clicking the device's name hyperlink. The Chassis View tab for the device appears.

**Step 3** In the right pane, click the **Configuration** sub-tab.

**Step 4** Expand the **General** area, and then enter the details of the device such as the node name, node alias, and select the location where you want to provision the device.

- Step 5** Set up the synchronization time for the device to synchronize with its associated controllers. You can either use the NTP/SNTP server time or set up a manual date and time for synchronization.
- Step 6** Check the **Enable Manual Cooling** check box to manually change the cooling profile of the device. The cooling profile allows you to control the speed of the fans in the device's shelf.
- Step 7** Click **Apply**. The changes in the settings are updated in the CTC.
- Step 8** Expand the **Network** area, select the network setting you want to modify, and then click the edit icon at the top left of the **Network** area. The **Edit Network General Settings** window appears.
- Step 9** Modify the required settings, and then click **Apply**.
- Note** You cannot modify the Node Address, Net/SubnetMask Length, Mask, and MAC Address of the device.
- Step 10** Configure security settings for a device. See [Create and Manage Users and User Logins for a Device, on page 321](#).
- Step 11** Configure the origination (TX) and termination (RX) patchcords for a device. See [Configure Patchcords for a Device, on page 322](#).
- Step 12** Configure the alien wavelength for a device. See [Configure GMPLS and WSON Properties, on page 329](#).
- 

## Create and Manage Users and User Logins for a Device

Use this procedure to create users and assign roles to manage a device. You can also view the list of users who are accessing the device at a time.

---

- Step 1** From the left sidebar, choose **Configuration > Network Devices**.
- Step 2** Select the device that you want to configure by clicking the device's name hyperlink. The Chassis View tab for the device appears.
- Step 3** In the right pane, click the **Configuration** sub-tab, and then expand the **Security** area.
- Step 4** In the **Users** tab, click the + icon to add a user.
- Step 5** Enter the user name.
- Step 6** From the **Security Level** drop-down list, choose one of the following options:
- **Retriever**—Users with this security level can view and retrieve information from the device, but cannot modify the configuration.
  - **Maintenance**—Users with this security level can retrieve information from the device and perform limited maintenance operations such as card resets, Manual/Force/Lockout on cross-connects or in protection groups, and BLSR maintenance.
  - **Provisioning**—Users with this security level can perform all maintenance operations and provisioning actions except those that are restricted to super users.
  - **Super User**—Users with this security level can perform all provisioning user actions, plus creating and deleting user security profiles, setting basic system parameters such as time, date, node name, and IP address, and doing database backup and restoration.
- Step 7** Enter your password, and then click **Save**. The user is added to the Users table.
-

You can select a user to edit or delete the user. However, you cannot edit the user name. Moreover, you cannot delete a user who has added the device to Cisco EPN Manager .

In the Security area, click the **ActiveLogins** tab to view the list of users who have logged in to the device using CTC, TL1 session, or Cisco EPN Manager . You can choose to logout a user or multiple users when the maximum login sessions for a device is reached.

## Configure Patchcords for a Device

The client card trunk ports and the DWDM filter ports can be located in different nodes or in the same single-shelf or multi-shelf node. A virtual link is required between the client card trunk ports and the DWDM filter ports. The internal patchcords provide virtual links between the two sides of a DWDM shelf, either in single-shelf or multishelf node. The patchcords are bidirectional, however, each direction is managed as a separate patchcord.

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

This procedure explains how to configure internal patchcords using the Chassis View using ANS (automatic node setup) for WDMs (wavelength division multiplexing). You can use the Chassis View to create and delete these internal patchcords. To configure origination (TX) and termination (RX) patchcords for a device:

- 
- Step 1** From the left sidebar, choose **Configuration > Network Devices**.
  - Step 2** Select the device that you want to configure by clicking the device's name hyperlink. The Chassis View tab for the device appears.
  - Step 3** In the right pane, click the **Configuration** sub-tab, and then expand the **Internal.patchcord** area.
  - Step 4** Click the + icon, and then choose the required origination (TX) and termination (RX) patchcords for the device.
  - Step 5** Click **Finish**. The patchcords are added to the Internal Patchcords table.
- 

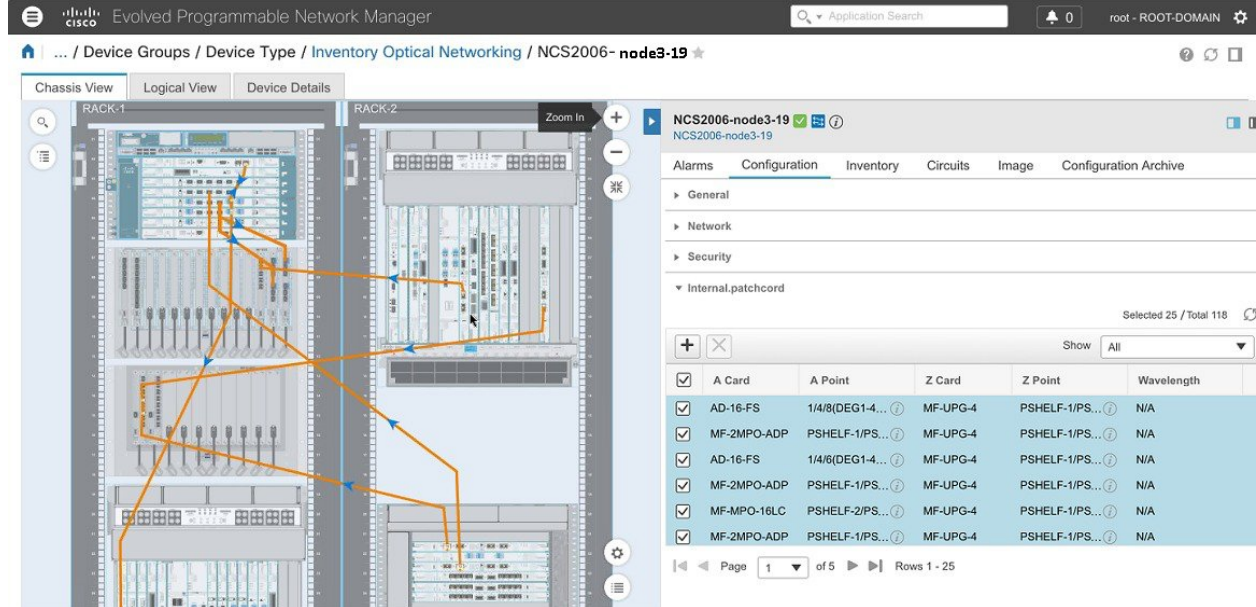
**Note**

Once you have created the patchcord, you cannot modify it. However, you can delete it.

You can select a patchcord or multiple patchcords in the Internal Patchcords table to view the direction of the patchcords in the Chassis View of the device, which is displayed in the left pane (as shown in the figure



below).



## Configure a Protection Group for a Shelf in a Device

Use this procedure to create a protection group for a shelf in a device.



**Note** You cannot configure a protection group for a rack.

### Before you begin

Following are the prerequisites before creating a protection group for a shelf:

- To create a Y Cable protection group, ensure that two cards of the same type that are configured with client ports are plugged in to the same shelf.
- To create a Splitter protection group, ensure that at least one OTU2XP card that is configured with trunk port 3-1 and trunk 4-1, is plugged in to the shelf.

- Step 1** From the left sidebar, choose **Configuration > Network Devices**.
- Step 2** Select the device that you want to configure by clicking the device's name hyperlink. The Chassis View tab for the device appears.
- Step 3** Expand the Chassis View Explorer, and then select the shelf for which you want to configure the protection group.
- Step 4** In the right pane, click the **Configuration** sub-tab, and then expand the **Protection** area.
- Step 5** Click the + icon to open the Create Protection Group window.
- Step 6** From the Type drop-down list, choose one of the following protection type:
  - **Splitter**—This protection type is applicable only when a MXPP/TXPP card is used. These cards provides splitter (line-level) protection (trunk protection typically on TXPP or MXPP transponder cards).

- **Y Cable**—This protection type is applicable only when two transponder or two muxponder cards that are configured with client ports, are plugged in to the same shelf in a device.

**Step 7** Choose a protect port and a working port for the shelf.

**Note** You will be able to select these ports only if you have completed the prerequisites listed at the beginning of this procedure.

**Step 8** Choose if the protection type is uni-directional or bi-directional. In the bidirectional mode, a failure on a active interface triggers a switchover of the traffic from the active interface to the protecting/backup interface.

**Step 9** Click the **Revertive** toggle radio button to revert the shelf from the protected port to the original port after the failure is fixed.

**Step 10** Choose the hold off time in mili seconds. Hold off time is the period that the shelf on the protected port must wait before switching to the original port after the failure is fixed. The shelf can revert to the original port after the hold time expires. The minimum value of hold off time must be 0.5.

**Step 11** Click **Apply**. The protection group is added to the Protection table.

## Configure Slices

Using Cisco EPN Manager you can configure the slice by controlling the bitrate on the client and trunk ports and by configuring the FEC and encryption types for each slice.

You must configure the five client ports of the slice at the same bitrate. Also, ensure that both trunk ports are always set to the same FEC mode.

To configure the slice:

**Step 1** Launch the **Chassis View** as described in [Open the Chassis View, on page 72](#).

**Step 2** Click the **Configuration** tab from the window displayed on the right.

**Step 3** Expand the **Slice Configuration** sub-tab.

**Step 4** To add new slice configuration, click the + (Add) button and specify the following details:

Slice Configuration Parameters	Descriptions
Slice Number	Numerical value that represents the Slice ID. You can create only one set of configuration per slice.
Client Bitrate	Total number of bits per second (in kilobits per second) to be configured on the client ports of the slice.
Trunk Bitrate	Total number of bits per second (in kilobits per second) to be configured on the trunk ports of the slice.
FEC	FEC value to be set on the trunk ports.  Before changing the FEC mode setting, ensure that the admin state of the interface you are trying to modify is in Down (out of service) state with G709 configuration enabled.
Encryption	Configures the slice to function with encrypted or unencrypted traffic.

**Step 5** Click **Apply** to deploy the changes to the device immediately.

You can add only one set of parameters per slice and not all parameters are editable once saved. To edit the parameters, delete the configuration for the slice and add it again.

## Configure Controllers (Optics, OTS, OCH, DSP, and DWDM)

Using Cisco EPN Manager , you can configure optical device controller parameters such as the wavelength, FEC, SD and SF BER reporting and thresholds, and more for controllers of type OTS, OTS OCH, DWDM, and more.

The Optical Transport Section (OTS) controller holds all the optical parameters for the OTS optical interfaces. The optical interface has different capabilities depending on its hardware components such as VOA and amplifier. Hence, the parameters enabled or disabled on the OTS controller depend on the actual hardware capability on the specific optical interface. You can configure parameters such as amplifier gain range, amplifier tilt, and OSRI for the OTS controller.

The Optical Transport Section OCH (OTS OCH) controller represents the OCM device available on the OTS optical interface. This controller has channel granularity over the OTS interface. The OTS OCH controller contains the wavelength information. You can configure only the admin status for the OTS OCH controller.

To ensure that you complete the slice configuration before configuring the controllers, see, [Configure Slices, on page 324](#).

To configure the optical controller parameters:

**Step 1** Launch the **Chassis View** as described in [Open the Chassis View, on page 72](#).

**Step 2** Click the **Configuration** tab from the window displayed on the right.

**Step 3** Expand the **Controllers** sub-tab. Depending on your device selection, supported tabs are displayed.

**Step 4** To edit the configuration on optical controllers, click **Optics**, choose the required settings, and click the modify icon to make your changes.

**Step 5** To edit the configuration on OTS controllers, click **OTS**, choose the required settings, and click the modify icon to make your changes.

**Step 6** To edit the configuration on OTS-OCH controllers, click **Ots-Och**, choose the required settings, and click the modify icon to make your changes.

**Step 7** To configure coherent DSPs, click **Coherent DSPs**, choose the required settings, and click the modify icon to make your changes.

Note that you cannot edit any parameter when the transport admin status is set to IS.

**Step 8** To edit the configuration on DWDM controllers, click **DWDM**, choose the required settings, and click the modify icon to make your changes.

Category	Parameters	Description
Common Optics, OTS-OCH, DSP, and DWDM	<ul style="list-style-type: none"> <li>Name</li> <li>Admin Status</li> <li>Operational Status</li> </ul>	<p>Name- (Display only) Displays the port number.</p> <p>Admin Status- Defines whether the interface is managed (Up), down, or in maintenance mode. You cannot modify the controller properties when the status of the interface is Up.</p>

Category	Parameters	Description
Controller Parameters	<ul style="list-style-type: none"> <li>Transport Admin Status</li> </ul>	<p>Operational Status – Defines whether the interface is operational and is performing as provisioned.</p> <p>Transport Admin Status – Defines the transport administration state of the controller.</p>
Common Optics and DWDM Parameters	Actual Wavelength (nm)	Displays the actual wavelength utilized by the channel.
-	Wavelength (nm)	Displays the wavelength value configured on the channel. Once the device Inventory Collection status is completed, the Actual Wavelength and Wavelength values will match.
-	FEC Mode	<p>FEC value to be set on the controllers.</p> <p>Before changing the FEC mode setting, ensure that the admin state of the interface you are trying to modify is in Down (out of service) state with G709 configuration enabled.</p>
Optics Parameters	Speed	Set the speed values (in Gigabits per second) that the controllers must operate on.
-	Differential Modulation	Enable or disable Differential Encoding (DE) based on the configured speed values.
-	Loopback	<p>Configure the loopback as:</p> <ul style="list-style-type: none"> <li>Internal - All packets are looped back internally within the router before reaching an external interface. It tests the internal Rx to Tx path and stops the traffic to egress out from the Physical port.</li> <li>Line - Incoming network packets are looped back through the external interface.</li> </ul>
-	SD BER	Set the signal degrade bit error rate. Your options are E-5, E-6, E-7, E-8, or E-9.
-	SF BER	Set the signal fail bit error rate. Your options are E-3, E-4, or E-5.
DWDM Parameters	Loopback	<p>Configure the loopback as:</p> <ul style="list-style-type: none"> <li>Internal - All packets are looped back internally within the router before reaching an external interface. It tests the internal Rx to Tx path and stops the traffic to egress out from the Physical port.</li> <li>Line - Incoming network packets are looped back through the external interface.</li> </ul>
-	<ul style="list-style-type: none"> <li>OTU-SD</li> <li>OTU-SF</li> <li>ODU-SD</li> </ul>	<p>Configure SF (signal fail) and SD (signal degrade) BER reporting and thresholds.</p> <p>Depending on whether the alarm is an OTU or ODU alarm, the alarm represents that SM BER is in excess based on the SD BER threshold or SF BER threshold.</p>

Category	Parameters	Description
	• ODU-SF	
OTS Parameters	Port Role	Current operational state of the port.  In case of a protection switch, the Com work role is displayed, whereas, in case of an amplifier module, the Com Line/Osc or Com Check role is displayed.
-	Rx/Tx Low Threshold (dBm)	Configures the receiver/transponder low receive power threshold. The valid range is from -500 to 300.
-	Ampli Channel Power (dBm)	Configures the amplifier per channel power set point. The valid range is -500 to 300. The default value is 0.0.
-	Channel Power Max Delta (dBm)	Configures the maximum difference among all the measured channel powers. The valid range is from 0 to 200.
-	Ampli Gain and Ampli Gain Range	Configures the amplifier gain set point. The valid mode for the range is normal or extended.  Note: The amplifier gain range is configurable only when the controller is in shutdown state.
-	Ampli Safety Controller Mode	Configures the safety control mode as auto or disabled.
-	OSRI	Configures the optical safety remote interlock as on or off.
-	Ampli Tilt	Configures the amplifier tilt using a number between -50 to +50.

**Step 9** Click **Apply** to deploy your changes to the device immediately.

**Step 10** (Optional) To change the unit of the DWDM grid value to either wavelength or frequency, go to **Administrator > Settings > System Settings > Circuits/VCs Display**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Terahertz (THz))**.

## Configure Passive Units

Passive units are passive cards provisioned using Cisco EPN Manager for optical devices. Cisco EPN Manager maintains these passive units in its database and does not deploy them to devices. Once configured, you can view these passive units in the Device Details and Inventory pages and use them to create managed links in the Network Topology.

To add and delete passive units:

### Before you begin

Ensure that you have either 'Administrator' or 'Config Manager' user privilege before you perform this task.

**Step 1** Launch the **Chassis View** as described in [Open the Chassis View, on page 72](#).

- Step 2** Click the **Configuration** tab from the window displayed on the right.
- Step 3** Expand the **Passive Units** sub-tab.
- Step 4** To add a passive unit click the Add (+) icon and specify the following details:
- Equipment ID: Choose the unique identifier for the passive unit. You can add up to 9 passive units per device.
  - Equipment Type: Choose the equipment type that determines if the slot is provisioned as a 48-channel muxponder/demuxponder or as an odd/even unit. Your options are **CME**, **ODDE**, and **EVEN**.
  - (Optional) Serial Number: Serial number that is unique to each passive unit. Cisco EPN Manager does not deploy this configuration to the device and maintains it only in its database.
- Step 5** Click **Apply** to deploy your changes to the device.
- Step 6** (Optional) To verify successful creation of the passive units, navigate to the Interfaces tab or to the Device Details tab and use the Interface Name filter to locate the passive units.
- The naming convention used for the passive units is:
- PUnit<number of the card> <equipment ID of the passive unit>*
- For example, *PUnit/1/16*.
- Step 7** To edit the configuration of the passive units delete them and configure the details again using the same equipment ID.
- Step 8** To delete the passive units, select the required passive unit and click the Delete (X) icon. Passive units associated with links can also be deleted. This causes the links to switch to the Partial state.
- Step 9** (Optional) To configure manual links using these passive ports, navigate to the network topology and create the links as described in [Manually Add Links to the Topology Map, on page 156](#).

## Edit Amplifier Module Settings on Optical Cards

You can modify the settings of amplifier modules inserted in optical slots of your device by changing the grid modes, node types, and UDC Vlan settings.

To edit the amplifier module settings:

### Before you begin

Ensure that you have either 'Administrator' or 'Config Manager' user privilege before you perform this task.

- Step 1** Launch the **Chassis View** as described in [Open the Chassis View, on page 72](#).
- Step 2** Click the **Configuration** tab from the window displayed on the right.
- Step 3** Expand the **Amplifier Module Settings** sub-tab.
- Step 4** Select the settings that you want to edit, click the Edit icon, and specify the following parameters:
- Grid Mode: Defines the optical spectrum on the interfaces of the amplifier module.
  - Node Type: Defines the type of the node in which the amplifier is set to work. Your options are: Terminal, Line, and Not Set.
  - Udc Vlan: Defines the VLAN associated to the selected slot and its UDC port.
- Note** Ensure that the Udc Vlan that you specify is unique on the device. Duplicate values are not supported.

**Step 5** Click **Apply** to deploy your changes to the device.

---

## Configure GMPLS and WSON Properties

### GMPLS UNIs:

The Generalized Multiprotocol Label Switching (GMPLS) User Network Interface (UNI) creates a circuit connection between two clients (UNI-C) of an optical network. This connection is achieved by signaling exchanges between UNI Client (UNI-C) and UNI Network (UNI-N) nodes, where UNI-C nodes are router nodes and UNI-N nodes are optical nodes.

GMPLS UNI is supported only on the 100G and 200G trunk ports of the Cisco NCS 1002 node. The prerequisite for the OCH trail circuit is to create a Link Management Protocol (LMP) link between the optical channel Add/Drop NCS 2000 series interface on the NCS 2000 series node and the NCS 1002 interface on the NCS 1002 node.

UNI is divided into client (UNI-C) and network (UNI-N) roles. A UNI-C network element requests and accepts circuit provisioning information. A UNI-N network element is the node adjacent to the UNI-C node and accepts and transports circuit provisioning information across the core network.

For UNI circuit provisioning, the network must meet the following requirements:

- An NE must be configured in as UNI-C and connected to a UNI-N NE.
- An NE must be configured as UNI-N and connected to a UNI-C NE.

### Static UNIs:

Link Management Protocol (LMP) is a logical link that is created on the trunk optics controller on the source and destination nodes of the tunnel. You can create static LMP links (Static UNIs) between the ports of two different devices. For example between a Cisco NCS 2000 series node and a Cisco NCS 1002 node. This then helps configure an LMP neighbor for a GMPLS UNI tunnel.

While configuring a Static UNI using Cisco EPN Manager, the RX Port and TX Port that you choose identify the card, shelf, or slot that you want participating in the UNI. While the RX Port represents the source for the UNI, the TX Port represents the destination.

Use the Remote Device field to specify the management IP address of the selected node. Use the Remote Client Interface field to choose the LMP link IP address of the optics controller.

### Alien Wavelength:

Use the Alien Wavelength tab to view and configure the port and wavelength parameters for the alien wavelength. You can also specify the required alien wavelength type, trunk mode and the forward error correction (FEC) mode.

### Fiber Attributes:

You can configure the parameters used during creation of the GMPLS UNI by configuring values such as the fiber type (by choosing Dispersion-Shifted (DS), True-Wave Classic (TWC), or other values). You can also specify the fiber length and specify the Polarization Mode Dispersion fiber coefficient.

The Attenuator In value identifies the input optical attenuation in dB between the node output port (for example, a LINE-TX port) and the input parameter of the fiber. Similarly, the Attenuator Out value identifies the same between the node input port (for example, a LINE-RX port) and the output parameter of the fiber.

You can choose the Channel Spacing value that configures the minimum frequency spacing between two adjacent channels in the optical grid. To specify the maximum number of channels expected on the span use the Channel Number field. Ensure that the channel number and channel spacing values are consistent. For example, there cannot be 80 channels with 100 GHz spacing.

To configure GMPLS/WSON parameters:

- Step 1** Launch the **Chassis View** as described in [Open the Chassis View, on page 72](#).
- Step 2** Click the **Configuration** tab from the window displayed on the right.
- Step 3** To configure these parameters, navigate to the paths described in the table below.

Task	Navigation	Description
Configure fiber attributes	GMPLS/WSON sub-tab > Fiber Attributes	Specify the fiber side, type, length, validation, channel spacing, channel number, and domain values. You can optionally also specify the attenuator (in and out) values.
Create and edit static UNIs	GMPLS/WSON sub-tab > Static UNIs	<ul style="list-style-type: none"> <li>• Add the RX and TX port remote controllers that must participate in the UNI.</li> <li>• The Remote Device field specifies the management IP address of the node.</li> <li>• The Remote Client Interface field specifies the link IP address of the controller.</li> </ul>
Create and edit GMPLS UNIs	GMPLS/WSON sub-tab > GMPLS UNIs	<ul style="list-style-type: none"> <li>• Specify the ingress and egress ports for the GMPLS UNI and choose if the UNI is of type numbered or unnumbered. Ensure that you specify if the UNI is of type UNI-C or UNI-N.</li> <li>• The trunk values are automatically configured to the respective alien wavelength values depending on your GMPLS UNI configuration. If the configured alien wavelength is supported on both trunk ports, then setting it on one of the trunk ports automatically configures the same alien wavelength on both trunk ports.</li> <li>• For Cisco NCS 2000 devices, the GMPLS UNI trunk value can be set to Default.</li> <li>• Specify the local and remote interface IP, and remote system IP and controller. These values enable the remote system connection for the UNI.</li> </ul> <p><b>Note</b> You can only specify remote system IPs of devices that are managed by Cisco EPN Manager .</p>
Configure Alien Wavelength parameters	GMPLS/WSON sub-tab > Alien Wavelength	Specify the required alien wavelength type, trunk mode and the FEC mode.

- Step 4** Make your changes and click **Save**.



**Step 5** To edit the values once configured, select the values and click the Edit icon in the toolbar. Make your changes and click **Save**.

For information on LMP link creation, see, [Optical Channel \(OCH\) Trail User-to-Network Interface \(UNI\)](#), on page 422.

---

## Configure Optical Cards

- [Configure Cards from the Chassis View](#), on page 331
- [Reset a Card](#), on page 332
- [Delete a Card](#), on page 332
- [Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC](#), on page 334
- [Configure cards: OTU2-XP, MR-MXP, WSE, AR-XPE, AR-XP, AR-MXP, 40E-MXP-C, and 40ME-MXP-C](#), on page 333
- [Configure SONET and Flex Line Cards](#), on page 337
- [Edit and Delete Pluggable Port Modules and Card Mode Configuration](#), on page 340
- [Cards and Supported Configuration for Cisco NCS 2000 Devices](#), on page 341

## Configure Cards from the Chassis View

This procedure adds a card to Cisco EPN Manager using the Chassis View. After adding the card, you can configure it by following the procedure in the relevant topic for that card type. Normally this is done before you physically add the card to the slot.

### Before you begin

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

---

**Step 1** Launch the Chassis View as described in [Open the Chassis View](#), on page 72.

**Step 2** Select the slot to which you want to add the card by doing one of the follow:

- Select the empty slot from the physical Chassis View, then click the **Add Card** link in the slot pop-up window.
- Use the Chassis View explorer to navigate to the empty slot, hover your mouse cursor over the "i" icon next to the slot, then click the **Add Card** hyperlink in the informational popup window.

Cisco EPN Manager highlights the slot in the physical Chassis View (indicating it is preprovisioned) and lists all of the cards that are supported by that device type.

**Note** Make sure the card you select is appropriate for the physical slot type.

**Step 3** Locate the card you want to add, then click **Add**. Cisco EPN Manager displays a status message after the card is added.

**Step 4** If you want to configure the card right away, click **Configure Now** in the status popup message. Otherwise, click **Ignore**.

---

## Delete a Card

When you delete a card, Cisco EPN Manager removes all information about the card including the card operating mode configuration associated with the card. When you add this card again at a later point of time, this information is not restored.

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

To delete a card from Cisco EPN Manager :

### Before you begin

Before you delete a card, make sure that:

- The associated payload values and card operating modes are deleted.
- The card does not have any active configuration running on the card (you will not be able to restore the configuration when you re-add the card).

---

**Step 1** Launch the Chassis View as described in [Open the Chassis View, on page 72](#).

**Step 2** Select the slot from which you want to delete the card by doing one of the follow:

- Select the card in the slot from the physical Chassis View, then click the **Delete Card** link in the pop-up window.
- Use the Chassis View explorer to navigate to the card, hover your mouse cursor over the "i" icon next to the card, then click the **Delete Card** hyperlink in the popup window.

Cisco EPN Manager highlights the slot in the physical Chassis View (indicating it is preprovisioned) and once you delete all cards of a slot, the slot is left blank in the Chassis View.

After you delete a card, Cisco EPN Manager performs an inventory collection for the node.

---

## Reset a Card

Resetting a card repositions the card in the chassis, which is similar to performing a sync operation. Cisco EPN Manager does not modify any configuration changes, and instead saves the settings and triggers an inventory collection.

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

To reset a configured card:

---

**Step 1** Launch the Chassis View as described in [Open the Chassis View, on page 72](#).

**Step 2** Select the slot from which you want to delete the card by doing one of the follow:

- Select the card in the slot from the physical Chassis View, then click the **Reset Card** link in the pop-up window.

- Use the Chassis View explorer to navigate to the card, hover your mouse cursor over the "i" icon next to the card, then click the **Reset Card** hyperlink in the popup window.

Cisco EPN Manager highlights the slot in the physical Chassis View (indicating it is preprovisioned). After you reset the card, a sync is performed and inventory collection is triggered.

---

### What to do next

Configure the properties of the card as described in [Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC, on page 334](#).

## Configure cards: OTU2-XP, MR-MXP, WSE, AR-XPE, AR-XP, AR-MXP, 40E-MXP-C, and 40ME-MXP-C

To configure card operating modes and PPMs:

### Before you begin

OTU2-XP and 40E-MXP-C cards can be configured with PPM directly without having to set the card operating mode. However, if you want to configure card operating modes for other cards you can perform this configuration directly via Cisco Transport Controller.

- Ensure that the device sync is complete and that the device's inventory collection status is 'Managed' or 'Completed'.
- Every time you add or delete a PPM, reactive inventory collection is triggered, and the device begins the sync process. Ensure that you wait for reactive inventory collection to complete before you deploy further configuration changes to the device. When the device sync is in progress, the deploy of PPM configuration changes to the device will fail.
- Once the card operating modes are configured, ensure that the device sync is completed. If not, Cisco EPN Manager will not be able to display the right Payload values for the selected cards.
- Ensure that granular inventory is enabled for all cards before performing any configuration changes on the cards.
- For all supported cards except 40E-MXP-C, 40ME-MXP-C, and OTU2-XP cards, you must first configure the card operating modes using Cisco Transport Controller and then return to Cisco EPN Manager to proceed with the following steps.

- 
- |               |                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Configuration &gt; Network Devices</b> .                                                                                                                                                                           |
| <b>Step 2</b> | Select the device that you want to configure by clicking the device's Name hyperlink to launch the device's Chassis view. This feature is supported only on Cisco NCS 2000 devices.                                          |
| <b>Step 3</b> | Use the <b>Chassis Explorer</b> to select the card that you want to configure.                                                                                                                                               |
| <b>Step 4</b> | Click the <b>Configuration</b> sub-tab from the window displayed on the right.                                                                                                                                               |
| <b>Step 5</b> | Navigate to the CTC tool and configure the operating modes for the cards. Card mode configuration is not supported on: OTU2-XP, MR-MXP, WSE, AR-XPE, AR-XP, and AR-MXP cards. For all other cards on Cisco NCS 2000 devices, |

configure card operating modes as described in [Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC, on page 334](#).

- Step 6** Expand the **Pluggable Port Modules** section to configure port modules and their respective payload values.
- Step 7** Click the '+' (Add) icon in the **Port Modules** section to create port modules (PPMs).
- Step 8** Select the **PPM number** and then click **Save**. The PPM port is set to PPM (1 port) by default and cannot be modified.
- Note** The '+' (Add) button is disabled when the maximum number of PPMs for the selected card are created. You must create all available ports before you can continue to the next step.
- Step 9** Click the '+' (Add) icon in the **Pluggable Port Modules** section.
- Note** For some PPMs, the respective payload values may not be enabled. To enable it, complete the card mode configuration described in Step 5 above, and then try to re-configure the payload values.
- Step 10** Choose the **port number**, **port type**, and **number of lanes** that must be associated with the selected PPM. The Port Type (payload) can be set to any supported client signals described in Table 2 below.
- Note** If the specified Port Type (payload) is not supported for the selected card operating mode or PPM, then the changes are not deployed to the device successfully. Ensure that the Payload values you specify, are supported on the selected card. See Table 2 below for reference.
- Step 11** Click **Finish** to deploy your changes to the device.
- Step 12** (Optional) If your changes are not visible in the Cisco EPN Manager, it could be because more than one person is working on the same card mode configuration and the changes are not reflected dynamically. Click the Refresh icon within each section to view the most recent changes.
- If you encounter a deploy failure, navigate to the error logs folder `/opt/CSCOlumos/logs/config.log` for more details about the cause of the error.

## Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC

To configure card operating modes and PPMs:

### Before you begin

- Ensure that the device sync is complete and that the device's inventory collection status is 'Completed'. If the device sync is on, then the deploy of PPM configuration changes will fail.
- Card mode configuration is not supported on: OTU2-XP, MR-MXP, WSE, AR-XPE, AR-XP, and AR-MXP cards. To configure the card operating modes on these cards, please use the Cisco Transport Controller tool.
- Ensure that the device sync is complete and that the device's inventory collection status is 'Managed' or 'Completed'.
- Ensure that granular inventory is enabled for all cards before performing any configuration changes on the cards.

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Select the device that you want to configure by clicking the device's Name hyperlink to launch the device's Chassis view.
- Step 3** Use the **Chassis Explorer** to select the card that you want to configure.
- Step 4** Click the **Configuration** sub-tab from the window displayed on the right.
- Step 5** Expand the **Pluggable Port Modules** section to configure port modules and their respective payload values.
- Step 6** Click the '+' (Add) icon in the **Port Modules** section to create port modules (PPMs). Select the PPM number and then click **Save**. The **PPM Port** value is set to PPM (1 port) by default and cannot be modified.
- Note**
- The '+' (Add) button is disabled when the maximum number of PPMs applicable for the selected card are created. You must create the required number of PPMs for the selected card before proceeding to the next step. For 100G-CK-C cards, you only need to create at least one PPM before proceeding to the next step.
  - For 400G-XP-LC cards, ensure that the PPMs 11 and 12 are created before configuring the card operating modes described in the next step (although the card mode is being created for either of the trunk ports). Without PPMs 11 and 12, the configuration changes deployed to the device will fail.
  - This step is optional for 100G-LC-C, 100G-ME-C, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, and 100GS-CK-C cards.
- Step 7** Expand the **Card Operating Modes** section to configure operating modes for the selected card.
- Step 8** Click the '+' (Add) icon to display a list of supported card operating modes or click the Edit icon to modify existing card operating modes. For 10x10G-LC cards you can add up to 5 card operating modes (10 ports that can act as sets of client or trunk ports), whereas for all other cards, only a single card operating mode can be set, after which, the + (Add) button is disabled.
- Step 9** Select an operating mode from the panel on the left and make your changes to the parameters.

- Note**
- Some card operating modes are disabled based on the card's peer configuration. Click on the 'i' icon next to the operating modes to understand how they can be enabled. See Table 1 below to understand the peer card configuration required to enable these operating modes.
  - For MXP cards, ensure that the trunk, peer, and peer skip card configuration is in the order described below:

Card Operating Modes	Trunk Card	Peer Card	Peer Skip Card
MXP_200G	Slot 2	Slot 3	Slot 4
MXP_200G on ONS 15454 M6 devices	100GS-CK-LC or 200G-CK-LC card in slots 2 or 7.	Slots 3, 4 or 5, 6.	Slots 3, 4 or 5, 6.
MXP_200G on Cisco NCS 2015 devices	100GS-CK-LC or 200G-CK-LC card in slots 2, 7, 8, 13, or 14.	MR-MXP cards in adjacent slots.	MR-MXP cards in adjacent slots.
MXP_10x10G_100G	Slot 7	Slot 6	Slot 5
MXP_10x10G_100G on ONS 15454 M6 devices	100GS-CK-LC or 200G-CK-LC card in slots 2 or 7	MR-MXP cards in adjacent slots 3, 4 or 5, 6.	MR-MXP cards in adjacent slots 3, 4 or 5, 6.
MXP_10x10G_100G on Cisco NCS 2015 devices	100GS-CK-LC or 200G-CK-LC card in slots 2, 7, 8, 13, or 14.	MR-MXP cards in adjacent slots.	MR-MXP cards in adjacent slots.
MXP_CK_100G on ONS 15454 M6 devices	100GS-CK-LC or 200G-CK-LC card and the peer MR-MXP card need to be in adjacent slots 2-3, 4-5, 6-7.		
MXP_CK_100G on Cisco NCS 2015 devices	100GS-CK-LC or 200G-CK-LC card and the peer MR-MXP card need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.		

For 400G-XP-LC cards, you can configure the OTNXC card operating mode with trunk operating mode of M-100G/M-200G on both Slice 1 and Slice 2. Supported slice configuration is OPM-10G, OPM-10x10G, and OPM6X16GFC.

The trunk operating mode configured on one of the ports reflects automatically in the second OTNXC port. You will not be able to manually configure both ports. For example, when you configure M-200G on trunk 11 and update both slices, then values for trunk 12 are greyed out, however, M-200G is automatically configured on trunk 12.

**Step 10** Click **Save** to deploy your changes to the device.

**Step 11** Expand the **Pluggable Port Modules** section to configure the payload values for each PPM.

**Step 12** Click the '+' (Add) icon in the Pluggable Port Modules section.

**Note** For some PPMs, the respective payload values may not be enabled. To enable it, complete the card mode configuration described in Step 9 above, and then try to re-configure the payload values.

- Step 13** Choose the **port number**, **port type**, and the **number of lanes** that must be associated with the selected PPM. The Port Type (payload) can be set to any supported client signals described in the Table 1 below.
- Note**
- If the specified Port Type (payload) is not supported for the selected card mode or PPM, then the changes are not deployed to the device successfully. Ensure that the Payload values you specify, are supported on the selected card. See Table 1 for reference.
  - You can configure the number of lanes only on cards that allow payload values to be split. For all other cards, the Number of Lanes field is disabled.
- Step 14** Click **Finish** to deploy your changes to the device.
- Step 15** (Optional) If your changes are not visible in the Cisco EPN Manager , it could be because more than one person is working on the same card mode configuration and the changes are not reflected dynamically. Click the Refresh icon within each section to view the most recent changes.
- If you encounter a deploy failure, navigate to the error logs folder `/opt/CSColumos/logs/config.log` for more details about the cause of the error.
- 

## Configure SONET and Flex Line Cards

This procedure describes how you can use Cisco EPN Manager to modify the line card configuration on 10X10G-LC SONET cards and 400G-XP, 200G-CK-LC, and 100GS-CK-LC Flex cards.

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

To configure a SONET or Flex line card:

### Before you begin

- To configure SONET line cards, ensure that you select a card with the operating mode MXP10X10G and OC192 payload value.
- To delete the SONET or Flex line card configuration, you only need to delete the payload values associated with the selected card. This deletes the SONET or Flex configuration from the device automatically. To delete the payload values, use the Pluggable Port Modes area under the configuration sub-tab.
- While configuring the SONET or Flex line card configuration, if you want to change the Line card type from SONET to SDH, or make other similar changes, you must first ensure that the admin state of the device is set to OOS-Disabled. If the device state is not OOS-Disabled, the line configuration changes deployed to the device will fail.
- To configuring Flex line card configuration, ensure that the card operating modes for the card have been previously set. See [Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC, on page 334](#).

- 
- Step 1** Launch the Chassis View as described in [Open the Chassis View, on page 72](#).
- Step 2** Select the slot from which you want to configure the card by doing one of the follow:
- Select the card in the slot from the physical Chassis View using the zoom in and out options.
  - Use the Chassis Explorer view to navigate to the card and select it.

- Step 3** Click the **Configuration** sub-tab from the window displayed on the right.
- Step 4** Expand the **Line** section and choose the **SONET** or **Flex** sub-tabs.
- The supported cards for SONET configuration are only 10x10G-LC cards, and for Flex cards, it is 400G-XP, 200G-CK-LC, and 100GS-CK-LC cards.
- Step 5** Choose one of the following ways to edit the configuration:
- Select the SONET or Flex tab for configuration that you want to edit and click the Edit icon.
  - Click the inline parameters that you want to edit one by one within the rows of the table.
- Step 6** Make the required changes to the parameters described in the table below and click **Save** to deploy your changes to the device.
- While configuring SONET parameters:
- When you set the Type to SDH, the Sync Messages checkbox is automatically disabled and cannot be configured.
  - When you enabled the Sync Message checkbox, the Admin SSM option is disabled and set to null.
- While configuring Flex parameters:
- For 400G-XP-LC cards, Flex line cards can be configured only for trunk ports 11/12.
  - For 100GS-CK-LC cards, Flex line cards can be configured only for trunk port 2.



Table 19: SONET and Flex Line Configuration Parameters and Descriptions

Line Card Type	Line Card Configuration Parameters	Descriptions
SONET	Port Number	The port number of the SONET interface you are configuring.
	Port Name	Allows you to add a name for the SONET optical port.
	SD BER	Sets the signal degrade bit error rate.
	SF BER	Sets the signal fail bit error rate.
	Type	Defines the port as SONET or SDH.
	Provides Sync	When checked, the card is provisioned as an NE timing reference.
	Sync Messaging	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.
	Admin SSM In	<p>If the node does not receive an SSM signal, it defaults to synchronization traceability unknown (STU). Admin SSM allows you to override the STU value with one of the following:</p> <ul style="list-style-type: none"> <li>• PRS—Primary reference source (Stratum 1)</li> <li>• STS2—Stratum 2</li> <li>• TNC—Transit node clock</li> <li>• STS3E—Stratum 3E</li> <li>• STS3—Stratum 3</li> <li>• SMC—SONET minimum clock</li> <li>• ST4—Stratum 4</li> </ul>
Flex	Port	The port number of the Flex interface you are configuring.
	Gridless	<p>Enables or disables the gridless tunability feature on the selected card. When the feature is enabled, you can configure the frequency values on the card. Your options are:</p> <ul style="list-style-type: none"> <li>• Enabled- When selected, enables you to edit the frequency parameter for Flex.</li> <li>• Disabled- When selected, disables the frequency parameter for Flex.</li> </ul>
	Frequency	Specifies the frequency on the port of the 400G-XP, 200G-CK-LC, and 100GS-CK-LC cards in the range 191350 to 196100.

# Edit and Delete Pluggable Port Modules and Card Mode Configuration

## Before you begin

### Pre-requisites for deleting PPMs:

- Ensure that the PPMs are not part of any Active or Provisioned circuits.
- PPMs and their respective payload values must be deleted only in the order described in the procedure below. Ensure that you first manually delete client ports 1 to 10 before deleting associated PPMs.
- Ensure that device sync is completed and the device's inventory collection status is either 'Completed' or 'Managed'.

### Pre-requisite for deleting card operating modes:

- Ensure that the cards are not part of any Active or Provisioned circuits.
- For 400G-XP cards, PPMs 11 and 12 cannot be deleted. These PPMs are deleted automatically when the associated card operating mode is deleted.
- The peer card or skip card must not be in Active state. You can delete the peer or skip card associations using CTC and then retry deleting the card operating mode via Cisco EPN Manager. You can also try directly deleting the card from Cisco EPN Manager. For more information, see [Delete a Card, on page 332](#).

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Select the device that you want to configure by clicking the device's Name hyperlink to launch the device's Chassis view.
- Step 3** Use the **Chassis Explorer** to select the card with the configuration you want to delete.
- Step 4** Click the **Configuration** sub-tab from the window displayed on the right.
- Step 5** Expand the **Pluggable Port Modules** section to delete Pluggable Port Modules (PPMs).
- In the **Pluggable Port Modules** sub-section, select the associated payload values that you want to delete and click the 'X' (delete) icon.
  - Click **OK** to confirm. The changes are deployed to the device.
  - In the **Port Modules** sub-section, select the PPMs that you want to delete and click the 'X' (delete) icon.
  - Click **OK** to confirm. The changes are deployed to the device.
- Note** You must delete all payload values associated with a given PPM, before you can delete the PPM.
- Step 6** Expand the **Card Operating Modes** section to delete the card configuration.
- To edit the card mode configuration, ensure that you select only 400G-XP cards, and click the Edit icon to make your changes. For all other cards, the configuration can be edited only by deleting the card mode configuration and re-creating it with new values.
  - To delete the card mode configuration, select the required card mode configuration and click the 'X' (delete) icon.
  - Click **OK** to confirm. The changes are deployed to the device.
-

## Cards and Supported Configuration for Cisco NCS 2000 Devices

**Table 20: 100GS-CK-LC and 200G-CK-LC Cards: Supported Configuration**

Card Operating Modes	Trunk Card	Peer card	Peer Skip Card	Supported Payload Types
MXP_200G	100GS-CK-LC or 200G-CK-LC card in slots 2, 7, 8, 13, or 14.	MR-MXP cards in slots 3, 6, 9, 12 or 15.	MR-MXP cards in slots 4, 5, 10, 11 or 16.	100GE and OTU4 OTU4 is supported only for the 200G-CK-LC card. Regeneration of any 100 G configuration 10GE 10GE 100GE
MXP_10x10G_100G	100GS-CK-LC or 200G-CK-LC card in slots 2, 7, 8, 13, or 14.	10x10G-LC cards in slots 3, 6, 9, 12 or 15.	MR-MXP cards in slots 4, 5, 10, 11 or 16.	100GE and OTU4 OTU4 is supported only for the 200G-CK-LC card. Regeneration of any 100 G configuration 10GE 10GE 100GE
MXP_CK_100G	100GS-CK-LC or 200G-CK-LC card and the peer MR-MXP card need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.	N/A	N/A	100GE and OTU4 OTU4 is supported only for the 200G-CK-LC card. Regeneration of any 100 G configuration 10GE 10GE 100GE
RGN-100G	100GS-CK-LC or 200G-CK-LC card and the peer card 100GS-CK-LC or 200G-CK-LC need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.	N/A	N/A	100GE and OTU4 OTU4 is supported only for the 200G-CK-LC card. Regeneration of any 100 G configuration 10GE 10GE 100GE

TXP-100G	100GS-CK-LC or 200G-CK-LC	N/A	N/A	N/A
----------	---------------------------	-----	-----	-----

**Table 21: 100G-CK-C and 100ME-CKC Cards: Supported Configuration**

Card Operating Modes	Trunk Card	Peer card	Skip Card	Supported Payload Types
TXP-100G	100G-CK-C/ 100ME-CKC	N/A	N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE
RGN-100G	100G-CK-C/ 100ME-CKC card and the peer card  100G-LC-C/ 100G-ME-C/ 100G-CK-C/ 100ME-CKC need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.	N/A	N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE
MXP-2x40G	100G-CK-C/ 100ME-CKC	N/A	N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE

**Table 22: 100G-LC-C and 100G-ME-C Cards: Supported Configuration**

Card Operating Modes	Trunk Card	Peer card	Skip Card	Supported Payload Types
TXP-100G	100G-LC-C/ 100G-ME-C	N/A	N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE
RGN-100G	100G-LC-C/ 100G-ME-C card and the peer card 100G-LC-C/ 100G-ME-C/ 100G-CK-C/ 100ME-CKC need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.	N/A	N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE

Table 23: 10X10G-LC Cards: Supported Configuration

Card Operating Modes	Trunk Card	Peer card	Skip Card	Supported Payload Types
TXPP-10G	10x10G-LC	N/A	N/A	<p>OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON</p> <p>Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card.</p> <p>Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card.</p> <p>10GE-LAN Phy, OTU2</p> <p>10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G</p> <p>10GE, 10G FC</p> <p>10GE</p> <p>10GE, OTU2e</p>
TXP-10G	10x10G-LC	N/A	N/A	<p>OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON</p> <p>Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card.</p> <p>Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card.</p> <p>10GE-LAN Phy, OTU2</p> <p>10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G</p> <p>10GE, 10G FC</p> <p>10GE</p> <p>10GE, OTU2e</p>

MXP-10x10G	10x10G-LC card and the peer 100G-LC-C, 100G-ME-C, 100G-CK-C, 100ME-CKC, 100GS-CK-LC or 200G-CK-LC card need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.	N/A	N/A	<p>OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON</p> <p>Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card.</p> <p>Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card.</p> <p>10GE-LAN Phy, OTU2</p> <p>10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G</p> <p>10GE, 10G FC</p> <p>10GE</p> <p>10GE, OTU2e</p>
RGN-10G	10x10G-LC	N/A	N/A	<p>OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON</p> <p>Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card.</p> <p>Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card.</p> <p>10GE-LAN Phy, OTU2</p> <p>10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G</p> <p>10GE, 10G FC</p> <p>10GE</p> <p>10GE, OTU2e</p>
LOW - LATENCY	10x10G-LC	N/A	N/A	N/A

FANOUT - 10X10G	10x10G-LC	N/A	N/A	<p>OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON</p> <p>Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card.</p> <p>Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card.</p> <p>10GE-LAN Phy, OTU2</p> <p>10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G</p> <p>10GE, 10G FC</p> <p>10GE</p> <p>10GE, OTU2e</p>
-----------------	-----------	-----	-----	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

400G-XP-LC and MR-MXP cards of Cisco NCS 2000 devices can be configured with the following card operating mode and payload values:

- Payload types OTU2/OC192 are supported on MR-MXP cards,
- Payload types 16G-FC/OTU2 are supported on 400G-XP-LC cards,
- Slice operational mode OPM\_6x16G\_LC is supported on 400G-XP-LC cards.

## Discover and Configure MPLS LDP and MPLS-TE Links

Using Cisco EPN Manager you can configure Label Distribution Protocol (LDP) and MPLS-TE links in an MPLS network.

### MPLS LDP

LDP provides a standard methodology for hop-by-hop (or dynamic label) distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying IGP routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward labeled traffic across an MPLS backbone. Cisco EPN Manager enables you to configure the potential peers and establish LDP sessions with those peers to exchange information.

To configure LDP using Cisco EPN Manager you need to know the network address and interface of the device on which the LDP links must be configured and also subnet mask for the configured IP addresses.



**Note** Before configuring MPLS LDP, ensure that the LDP ID is pre-configured on the device.

### MPLS-TE

Cisco EPN Manager supports the provisioning of MPLS Traffic Engineering (MPLS-TE) services. MPLS-TE enables an MPLS backbone to replicate and expand the TE capabilities of Layer 2 over Layer 3. MPLS TE

uses Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP) across the backbone. For more information, see, [Supported MPLS Traffic Engineering Services, on page 428](#).

To configure LDP and MPLS-TE parameters:

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.

**Step 4** To configure LDP links:

- a) Choose **MPLS > LDP** and click '+' to specify new LDP parameters. To edit existing parameters, click the LDP Address hyperlink and click the Edit icon at the top right corner of the page.

**Note** You can only add a single set of LDP settings per device.

- b) Specify the LDP parameters described in the table below and click **Save** to deploy your changes to the device.

**Step 5** To configure MPLS-TE links:

- a) Choose **MPLS > MPLS-TE** and click the Edit icon at the top right corner of the page.
- b) Specify the MPLS-TE parameters described in the table below and click **Save** to deploy your changes to the device.

MPLS LDP Fields	Field Descriptions
LDP Interface	Choose the LDP interface that is the source loopback interface for the LDP session on the device.
LDP Address	Specify the IP address of the LDP interface. Once the LDP address is set, it cannot be edited. To change the LDP address, delete the LDP session and create a new session with the new LDP address.
Mask	Enter the network mask for the specified IP address in A.B.C.D format.
Discovery Hold time and Discovery Target Hold time	(Optional) Enter the time, in seconds, an LDP source and a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor. Range is 1 to 65535.
DownStream Min Label and DownStream Max Label	(Optional) Enter the minimum and maximum number of hops permitted in an LSP established by the Downstream on Demand method of label distribution. Range is 16 to 32767.
DownStream Max Hop Count	(Optional) Enter the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution. Range is 1 to 255.
IGP Hold Down Time	(Optional) Enter the time, in seconds, to specify the time for which the declaration of LDP sync state is delayed after session establishment upon link coming up. Range is 1 to 2147483647.
Explicit Null Enabled	(Optional) Enable this value to advertise explicit-null labels for the directly connected route. Values are Yes (enabled) or No (disabled).
Initial Back Off and Max Back Off	(Optional) Enter the initial and maximum back off delay value in seconds. Range is 5 to 2147483.



MPLS LDP Fields	Field Descriptions
NSR Enabled	Choose true or false to either enable or disable LDP nonstop routing (NSR). Enabling NSR allows the LDP to continue to operate across a node failure without losing peer sessions.
Entropy Enabled	Choose true or false to either enable or disable the MPLS LDP Entropy Label support feature which helps improve load balancing across MPLS networks using entropy labels.

Fields	Field Descriptions
MPLS TE Tunnel Enabled	Activates the display of the list of automatic bandwidth enabled tunnels, and indicates if the current signaled bandwidth of the tunnel is identical to the bandwidth that is applied by the automatic bandwidth
Auto Bandwidth Timer Frequency (Sec)	To set the interval (in seconds) at which the automatic bandwidth on a tunnel interface is triggered.
Reoptimize Timer Frequency (Sec)	Set the value (in seconds) to trigger the reoptimization interval of all TE tunnels.
Auto Backup Tunnel Enabled	To display information about automatically built MPLS-TE backup tunnels.
Backup Tunnel Min. Range and Backup Tunnel Max. Range	Configures the range of backup autotunnel numbers to be between the specified minimum and maximum value. Ensure that minimum range for the backup tunnel is lower than the maximum range.
SRLG Exclude	Specifies an IP address to get SRLG values from, for exclusion.
Un-numbered Interface	Enables IP processing on the specified interface without an explicit address.

### What to do next

Monitor LDP links on the Network Topology:

1. In the left sidebar, choose **Maps > Topology Maps > Network Topology**.
2. Click on the **Device Groups** button, select the required device group(s), and click **Load**.
3. Click **Show** in the topology toolbar and choose **Links**.
4. Select the **LDP** check box under Control Plane to display LDP links on the map.
5. Click on an LDP link to see details about the link.

For information on how to provision MPLS-TE services, see [Provision MPLS Traffic Engineering Services, on page 489](#).

# Analyze Ports Using SPAN and RSPAN

Using Cisco EPN Manager, you can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or to a monitoring device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. Traffic that enters or leaves source ports or traffic that enters or leaves source VLANs are monitored.

If you configure SPAN to monitor incoming traffic, then traffic that gets routed from another VLAN to the source VLAN cannot be monitored. However, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

Cisco EPN Manager allows you to configure only one Local SPAN session per device. Local SPAN sessions copy traffic from one or more source ports in any VLAN to a destination port for analysis.

Using Remote SPAN you can configure source ports, source VLANs, and destination ports on different switches, enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN.



## Note

To monitor ports, you must ensure that the ports are associated with one or more VLANs (source or destination).

To enable port monitoring (or mirroring):

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.

**Step 4** Configure an RSPAN session:

- a) Choose **Port Analyzer > RSPAN > Destination Node** to configure the destination node for RSPAN.
- b) Click '+' to specify the RSPAN session ID. To edit existing settings, click the session ID hyperlink and click the Edit icon at the top right corner of the page.

You can add up to 14 RSPAN and SPAN sessions.

- c) Choose a session ID and click **Save**.  
The session type Remote Destination (Remote RSPAN) is set by default and cannot be edited.
- d) Click the session ID hyperlink to specify the source and destination settings for the destination node.
- e) Click the **Source Settings** tab, choose a valid VLAN ID (auto populated based on the VLANs configured on the selected device), and click **Save**.

You can add only a single VLAN as the source for the destination node. If no VLANs are configured, you need to configure them and return to this step. See [Configure VLAN Interfaces, on page 299](#).

- f) Click the **Destination Settings** tab, select the interface that must act as the destination node for the RSPAN, and click **Save**.
- a) From the features panel, choose **Port Analyzer > RSPAN > Source Node** to configure the source node for RSPAN.

- b) Click '+' to specify common RSPAN source node settings. To edit existing settings, click the session ID hyperlink and click the Edit icon at the top right corner of the page.
  - c) Choose a session ID and click **Save**.
- The session type Remote Source (Remote SPAN) is set by default and cannot be edited.
- d) Click the session ID hyperlink to specify the source and destination settings for the source node.
  - e) Click the **Source Settings** tab, specify the following values, and click **Save**.

- i) In the **Interface** drop-down menu, choose the interface that will act as the source interface for the RSPAN source node.

An interface specified as a source node for RSPAN can also be used as the source/destination node for SPAN.

- ii) In the **Direction** drop-down menu, choose direction in which the interface must be applied to the RSPAN source node. Your options are:

- **Transmit**: monitors all packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that session. The copy is provided after the packet is modified.
    - **Receive**: monitors all packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that session.
    - **Both**: (default value) monitors a port or VLAN for both received and sent packets.

You can add multiple interfaces to the source node for RSPAN and then associate a single VLAN ID to these interfaces.

- f) Click the **Destination Settings** tab, choose a valid VLAN ID (auto populated based on the VLANs configured on the selected device), and click **Save**.

## Step 5

Configure a SPAN session:

- a) Click **Port Analyzer > SPAN**.
- b) Click the '+' to specify common SPAN source node settings. To edit existing settings, click the session ID hyperlink and click the Edit icon at the top right corner of the page.

Interfaces configured as the source and destination node for RSPAN, cannot be used for SPAN.

- c) Choose a session ID and click **Save**.
- The session type Local (Local SPAN) is set by default and cannot be edited.
- d) Click the session ID hyperlink to specify the source and destination settings for SPAN.
  - e) Click the **Source Settings** tab, and choose the interface and direction in which the interface must be applied for SPAN, and click **Save**. For more details, see Step 4.

An interface specified as a source node for RSPAN can also be used as the source/destination node for SPAN.

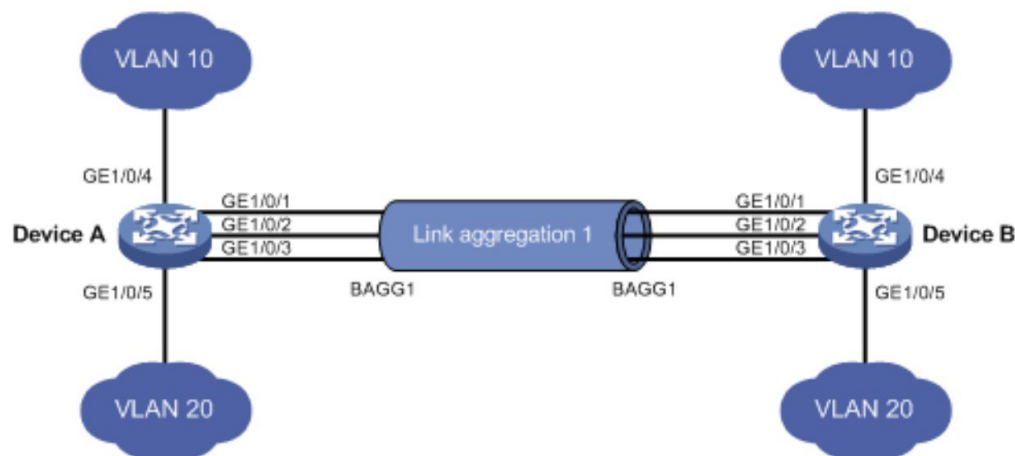
- f) Click the **Destination Settings** tab, choose a valid VLAN ID (auto populated based on the VLANs configured on the selected device), and click **Save**.
- g) (Optional) To verify that your changes were configured correctly, use the following command in your device CLI:

```
show monitor session all
```

# Configure and View Ethernet Link Aggregation Groups

An Ethernet Link Aggregation Group (LAG) is a group of one or more ports that are aggregated together and treated as a single link. Each bundle has a single MAC, a single IP address, and a single configuration set (such as ACLs). LAGs provide the ability to treat multiple switch ports as one switch port. The port groups act as a single logical port for high-bandwidth connections between two network elements. A single link aggregation group balances the traffic load across the links in the channel. LAGs help provision services with two links. If one of the links fails, traffic is moved to the other link.

The following figure illustrates a LAG created between two devices: Device A and Device B.



405431

Cisco EPN Manager allows you to view and manage LAGs in the following ways:

- [Create Link Aggregation Groups \(LAG\) Using Multiple Interfaces, on page 350](#)
- [View Ethernet LAG Properties, on page 351](#)

## Create Link Aggregation Groups (LAG) Using Multiple Interfaces

Using Cisco EPN Manager, you can create LAGs that provide the ability to treat multiple physical switch ports as a single logical one.

### Before you begin

- Only interfaces that are not already part of an existing LAG can be selected. An interface cannot be part of more than one LAG.
- The selected group of interfaces must all consist of the same bandwidth type.
- Inventory collection status for the devices that participate in the LAG must be *Completed*.

To create a LAG:

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **Interfaces > Link Aggregation**.
- Step 5** Depending on the type of control method that you want to use, click the **PAgP** or the **LACP** tab.
- Step 6** To create a new LAG, click the Add (+) sign.
- Step 7** Enter a unique name for the LAG. Ensure that the channel group ID that you specify is part of the LAG name. For example, for a channel group ID of 10, your LAG name should be:
- 'Bundle-Ether10' for Cisco IOS-XR devices.
  - 'Port-channel10' for Cisco IOS, Cisco ME3600, and Cisco ME3800 devices.
- Step 8** Enter a number between 1 to 16 to specify the Channel Group ID. The channel group ID ranges for different types of devices is: 1-8 for Cisco ASR 90X devices, 1-64 for Cisco ASR 920X devices, 1-26 for Cisco ME3x00 devices, 1-48 for Cisco NCS42xx devices, and 1-65535 for Cisco ASR9000 devices.
- Step 9** Click the **Member Port Settings** tab to specify the member port values:
- LACP Modes: LACP can be configured with the following modes:
    - Active- In this mode, the ports send LACP packets at regular intervals to the partner ports.
    - Passive- In this mode, the ports do not send LACP packets until the partner port sends LACP packets. After receiving LACP packets from the partner port, the ports then send LACP packets to the partner port.
  - PAgP Modes: PAgP modes can be configured with AUTO, DESIRABLE, or ON. For ASR9K devices, only On PAgP mode is enabled. ON implies that the mode is set to PAgP - manual.
- Step 10** Click **Save**.
- Your changes are saved and you can now add interfaces to the created LAG.
- Step 11** To add interfaces to the created LAG, select the required channel group from the Link Aggregation table and click the Edit icon.
- Step 12** Select the interfaces you want to use to create the LAG.
- Step 13** Click **Save**.
- The LAG is created using the interfaces you selected.
- 

## View Ethernet LAG Properties

You can view properties for Ethernet LAGs in the following ways:

- Using the Device Configuration tab:
  1. Go to **Network Devices > Device Properties > Configuration** tab.
  2. Select the device on which you want to configure the LAG by clicking the device name hyperlink.
  3. Click the **Configuration** tab, then click the **Logical View** left side tab.

4. Click **Interfaces > Link Aggregation** in the Features panel.

- Using the Device Details tab:

1. Go to **Network Devices > Device Properties**.
2. Select the device on which you want to configure the LAG by clicking the device name hyperlink.
3. Click the **Device Details** tab.
4. Click **Interfaces > Ether Channel** in the Features panel.

## Configure Routing Protocols and Security

Using Cisco EPN Manager, you can configure the following routing protocols for your CE and Optical devices. You can also configure security for your devices using ACLs.

Before you configure routing protocols and ACLs, ensure that the device's Inventory Collection status is 'Completed'.

To view a device's routing table, open the Device 360 view and choose **Actions > Routing Table Info > All**.

- [Configure BGP, on page 352](#)
- [Configure EIGRP, on page 355](#)
- [Configure an IS-IS, on page 356](#)
- [Configure OSPF, on page 358](#)
- [Configure RIP, on page 360](#)
- [Configure Static Routing, on page 361](#)
- [Configure ACLs, on page 361](#)

## Configure BGP

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) in your network. By configuring BGP, your device is enabled to make routing decisions based on paths, network policies, or rule-sets configured by a network administrator.

Using the Cisco EPN Manager, you can configure BGP routing and establish a BGP routing process by specifying the AS number and Router ID. You can then create a BGP neighbor which places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer. To configure the BGP neighbor, you need to provide the neighbor's IPv4 address and its peer AS number. BGP neighbors should be configured as part of BGP routing. To enable BGP routing, at least one neighbor and at least one address family must be pre-configured.

To view a device's BGP and BGP Neighbors routing table, open the Device 360 view, then choose **Actions > Routing Table Info**.

To configure BGP routing protocol on a device:

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Select the required device by clicking the device name hyperlink.

**Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.

**Step 4** Choose **Routing > BGP**.

**Note** The configuration changes on Cisco Catalyst 6500 Series devices with a quad-supervisor Virtual Switching System (VSS) are not dynamically reflected on this page. To view these changes, ensure that the 24 hour periodic device sync is completed. Alternatively, you can manually sync these devices with Cisco EPN Manager .

**Step 5** To configure the BGP routing process, click the + icon or if BGP is already configured, click the AS number hyperlink and then click the Edit icon to enter the BGP Process details described in the table below.

**Step 6** Click **Save** to deploy your changes to the device and to enable the BGP Address Family and BGP Neighbor tabs.

**Step 7** To configure the BGP address family details, click the **BGP Address Family** tab and choose the address family details described in the table below, and click **Save**.

**Step 8** To configure the BGP neighbor, click the **BGP Neighbor** tab and choose the neighbor device by selecting the device's IP address from the list.

**Step 9** To create a new BGP neighbor, click the Add (+) icon, specify the following details described in the table below.

**Step 10** Click **Save**. The updated BGP routing process values are saved and deployed to the selected device.

To verify that your changes were saved, go to **Configuration > Network Devices**, launch the Device Details page, and click the **Logical View** tab. Choose **Routing > BGP**. You can view your BGP configuration details such as the Neighbor Address, Remote AS, Address Family Type and Modifier, and Advertise Interval Time configured on the device.

Fields	Sub-field	Descriptions
Common BGP Process fields	AS Number	Enter the AS number using a numeric value from 1 to 4294967295.
	Router ID	<ul style="list-style-type: none"> <li>Enter the Router ID. The value can be an IPv4 or an IPv6 address of the format: <ul style="list-style-type: none"> <li>A.B.C.D- for IPv4 addresses, where A, B, C, and D are integers ranging from 0 to 255.</li> <li>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx - for IPv6 addresses, where x would be a hexadecimal value and where the address uses eight sets of four hexadecimal addresses (16 bits in each set), separated by a colon (:).</li> </ul> </li> </ul>
	Log Neighbor Changes	Select to track neighbor router changes.
BGP Address Family fields	BGP Global AF	<ul style="list-style-type: none"> <li>Address Family: Enter the BGP address family prefixes for the routing process. Your options are IPv4 and IPv6 (for unicast, multicast, and MVPN), VPNv4 and VPNv6 (for unicast), and IPv4 (for MDT).</li> <li>Allocate Label: Choose the labeled unicast address prefixes.</li> </ul>

Fields	Sub-field	Descriptions
		<ul style="list-style-type: none"> <li>Allocate Label Custom Policy Name: Choose a custom policy to be associated with the routing process.</li> </ul>
	BGP Additional Paths	<p>Specify the details for the paths that enable the advertisement of multiple paths through the same peering session for the same prefix without the new paths implicitly replacing any previous paths.</p> <ul style="list-style-type: none"> <li>Additional Paths: Choose whether the device must send, receive, or send and receive additional paths. This is done at the address family level or the neighbor level. During session establishment, the specified BGP neighbors negotiate the Additional Path capabilities (whether they can send and/or receive) between them.</li> </ul> <p><b>Note</b> While configuring Cisco CAT65000 devices, you can configure only Install as the additional path value.</p> <ul style="list-style-type: none"> <li>Best Value: This field is enabled only when the Additional Paths value that you choose supports the configuration of the Best Value field.</li> </ul>
	BGP Neighbor AF	<p>Specify the address family details that the specified BGP neighbor belongs to:</p> <ul style="list-style-type: none"> <li>Neighbor Address: Choose the Router ID of the neighboring router. These values are populated based on the BGP neighbors created in the Neighbor tab. The value can be an IPv4 or an IPv6 address of the format: <ul style="list-style-type: none"> <li>A.B.C.D- for IPv4 addresses, where A, B, C, and D are integers ranging from 0 to 255.</li> <li>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx - for IPv6 addresses, where x would be a hexadecimal value and where the address uses eight sets of four hexadecimal addresses (16 bits in each set), separated by a colon (:).</li> </ul> </li> <li>Send Label: Choose the type of label that must be associated with the neighbor.</li> <li>Route Reflector Client: Enable this field to configure the router as the route reflector and the specified neighbor as its client.</li> <li>AIGP: Select to enable the accumulated interior gateway protocol (AIGP) path attribute.</li> <li>Send Community: Choose how the community attributes must be sent to an external Border Gateway Protocol (eBGP) neighbor.</li> <li>Next Hop Self: Select to set the BGP next-hop attribute of routes being advertised over a peering session to the local source address of the session.</li> <li>Incoming and Outgoing Route Map Name: Choose to indicate whether a route policy must be applied to inbound or outbound updates from the neighbor.</li> </ul>
	BGP Network Mask	<ul style="list-style-type: none"> <li>Network Address and Mask: Specify the network IP address and network mask for the specified IP address.</li> </ul>



Fields	Sub-field	Descriptions
		<ul style="list-style-type: none"> <li>• Back Door Route: Enable to set the administrative distance on an external Border Gateway Protocol (eBGP) route to that of a locally sourced BGP route, causing it to be less preferred than an Interior Gateway Protocol (IGP) route.</li> <li>• Network Route Policy Name: Choose the route policy that will be used to select prefixes for label allocation. This enables BGP to allocate labels for all or a filtered set of global routes (as dictated by the route policy).</li> </ul>
BGP Neighbor tab fields	-	<p>Specify the following values:</p> <ul style="list-style-type: none"> <li>• Peer AS Number- Enter the value for the autonomous system number using integers in the range 1 to 4294967295.</li> <li>• Neighbor Address- Enter the IP address of the BGP neighbor that you want to configure. Only IPv4 address of the format A.B.C.D are supported.</li> <li>• Local AS Number and Action: Specifies an autonomous-system number to prepend to the AS_PATH attribute. The range of values is any valid autonomous system number from 1 to 65535.</li> <li>• Update Source: Use this option to establish a peer relationship (TCP connection) using the loopback interface as an alternative instead of using the interface closest to the peer router.</li> <li>• Fall-over: Select a value to enable the BGP fast peering session deactivation for improving the convergence and response time to adjacency changes with the specified BGP neighbor.</li> <li>• Password Encryption and Password: Specify whether password encryption is enabled or not, and if enabled, what the password value is.</li> <li>• (View only) Neighbor State: View the connection status of a neighbor device participating in a BGP routing process. The states are: Idle, Connect, Active, Opensent, Openconfirm, and Established.</li> </ul> <p>The neighbor device generates events only when its connection status is Established. Please check the connection status frequently in case there are updates from the device.</p> <p><b>Note</b> The neighbor state value is not updated during a granular inventory sync. To see the updated values, wait for the sync to end successfully.</p>

## Configure EIGRP

In EIGRP (Enhanced Interior Gateway Routing Protocol), when an entry in the routing table changes in any of the routers, it notifies its neighbors of only the change (rather than sending the entire routing table). Every router in the network periodically sends a “hello” packet so that all routers on the network understand the states of their neighbors. If a “hello” packet is not received from a router within a certain period of time, the router is considered inoperative.

EIGRP uses the Diffusing Update Algorithm (DUAL) to determine the most efficient route to a destination and provides a mechanism for fast convergence. If EIGRP and IGRP (Interior Gateway Routing Protocol) are being used on the same device, the protocols can interoperate because the routing metric used by one protocol is easily translated into the other protocol's metric.

To view a device's EIGRP and EIGRP Neighbors routing table, open the Device 360 view, then choose **Actions > Routing Table Info**.

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **Routing > EIGRP**.
- Step 5** Expand the **IPv4 EIGRP Routes** drop-down, click the Add (+) button, and enter the Autonomous System (AS) number, passive interface, and auto summary value that must be associated with the EIGRP routes.
- Step 6** Expand the **IPv6 EIGRP Routes** drop-down, click the Add (+) button to enter the following IPv6 values associated with the EIGRP routes. Depending on the type of device you select, this drop-down may be hidden. For example, for Cisco IOS-XR devices, you cannot specify IPv6 addresses.
- AS number- Enter the Autonomous System number that must be associated with the EIGRP route using a numeric value from 1 to 65535.
  - Administrative distance- Specify the distance that will be set for path selection. The available values are between 1 and 255.
  - Maximum paths- Specify the highest number of paths that can be used by the router for load balancing per route. You can set a numeric value between 1 and 32.
  - Router ID- Enter the identified for the router on which the EIGRP route must be configured. The router ID must be in the range 0.0.0.1 to 255.255.255.254.
  - Stub AS- Use true or false values to specify whether Stub Autonomous System must be associated with the EIGRP route.
- Step 7** Use the **Add/Remove Passive Interfaces** button for both IPv4 and IPv6 EIGRP routes to specify whether the loopback0 value must be associated with the specified interfaces. Depending on the type of device you select, this button may be hidden. For example, for Cisco IOS-XR devices, you cannot specify passive interfaces.
- Step 8** Click **Save** to deploy your changes to the device.
- 

## Configure an IS-IS

Intermediate System-to-Intermediate System (IS-IS) Protocol is an intra-domain OSI dynamic routing protocol which uses a two-level hierarchy to support large routing domains (administratively divided into areas). Routing within an area is referred to as Level 1 routing. Routing between areas is referred to as Level 2 routing. In order to enable IS-IS for IP on a Cisco router and have it exchange routing information with other IS-IS enabled routers, you must perform the following tasks:

- Enable the IS-IS routing process on the device and assign areas.
- Enable IS-IS IP routing on the required interfaces.

An interface with a valid IP address can be designated to act as a Level 1 (intra-area) router, a Level 1\_2 (both a Level 1 router and a Level 2) router, or a Level 2 (an inter-area only) routing interface for a given IS-IS

instance. After the IS-IS routing starts working across the routers between the designated interfaces, the IS-IS neighborhood is automatically generated.



**Note** To enable ISIS routing, at least one address family must be configured by default. In this release, configuring address families cannot be done using Cisco EPN Manager .

To configure the IS-IS process on a device:

**Step 1** Choose **Configuration** > **Network Devices**.

**Step 2** Select the device on which you want to configure the IS-IS routing protocol by clicking the device name hyperlink.

**Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.

**Step 4** Choose **Routing** > **IS-IS**.

**Step 5** To configure a new IS-IS process, click the '+' icon and enter the following parameters:

- Specify the process ID using alphanumeric characters only. No spaces or special characters are allowed.
- (Optional) Specify the Net ID in NSAP format. For example, your NET ID can be 49.0001.0000.0001.0010.00, where:
  - 49 - represents the first portion of the area ID which represents the AFI (Authority and Format Indicator).
  - 0001 - represents the second portion of the area ID.
  - 0000.0001.0010 - represents the system ID.
  - 00 - represents the N-selector which is always 0.
- Specify the type of IS-IS routing protocol. Your options are: Level 1, Level 2, and Level 1\_2.

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

**Step 7** To configure this routing process on the selected device's interfaces:

- a) Select the IS-IS protocol process created in the above steps from the **Routing** > **IS-IS** list.
- b) Click the IS-IS process ID hyperlink.
- c) Use the **IS-IS Interfaces** tab to specify the interfaces of the device on which the selected IS-IS configuration is to be applied:
  - Click the '+' icon to enter the interface details.
  - From the **Circuit Type** drop-down menu, select the type of circuit to which this configuration is to be applied. Your options are: Level 1, Level 2, and Level 1\_2.
  - From the **Interface** drop-down menu, select the required interfaces.
  - (Optional) Specify the Level 1 and Level 2 metric and priority values. For the **Priority** field enter a value between 1 to 127 and for the **Metric**, a value between 1 to 16777214.
  - Enable the **Point-to-Point** checkbox to enable point to point connection.
  - Click **Save** to deploy the configuration onto the selected interfaces.

**Step 8** Click **Save**. The selected IS-IS process is configured on the specified interfaces of the device.

**Step 9** (Optional) To view IS-IS neighbors associated with the selected device, click the IS-IS hyperlink and click the **IS-IS Neighbors** tab. You can view the configured neighbor's hostnames, IP addresses, system IDs, IS-IS types, their connection states, the configured hold down time values, and the local interface names.

**Note** If the hostnames of the IS-IS neighbors are greater than 15 unique characters, the hostnames are not displayed in Cisco EPN Manager. Ensure that the hostnames are not more than 15 unique characters.

**Step 10** (Optional) To delete IS-IS routing processes configured using Cisco EPN Manager :

- a) Go to **Configuration > Network Devices**, launch the Device Details page, and choose **Routing > IS-IS**.
- b) Select the required IS-IS process from the list.
- c) Click the 'x' icon to delete and click **OK** to confirm the delete operation.

## Configure OSPF

Open Shortest Path First (OSPF) is a standards-based routing protocol that uses the Shortest Path First (SPF) algorithm to determine the best route to its destination. OSPF sends Link State Advertisements (LSAs) to all routers within the same configured area. OSPF sends routing updates only for the changes in the routing table; it does not send the entire routing table at regular intervals.

Using Cisco EPN Manager you can configure OSPF for IPv4 and IPv6 addresses. To do this, ensure that you know the router ID, the administrative distance that you want to configure on the router, and the maximum path values to be set.

To configure the OSPF routing process:

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Select the device on which you want to enable OSPF by clicking the device name hyperlink. Select only IOS-XR devices.

**Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.

**Step 4** Choose **Routing > OSPF**.

**Note** The configuration changes on Cisco Catalyst 6500 Series devices with a quad-supervisor Virtual Switching System (VSS) are not dynamically reflected on this page. To view these changes, ensure that the 24 hour periodic device sync is completed. Alternatively, you can manually sync these devices with Cisco EPN Manager.

**Step 5** To add a new OSPF process, click the + sign. To modify existing OSPF processes, select the required process by clicking the process ID hyperlink and click the Edit icon at the top right corner of the page.

**Step 6** Specify the common OSPF parameters as described in the table below.

**Step 7** Click **Save**. Your configuration changes are saved. To verify, click the **Configuration** tab, choose **Routing > OSPF**, and view the displayed details.

**Step 8** Specify the **OSPF Interfaces** settings:

Once you have configured the OSPF process with basic properties, you can further deploy that configuration directly on an entire network or on an OSPF area. To do this, you need to specify the OSPF area ID, the device's interface details, the network type, etc. To change OSPF interface settings:

- a) Choose **Configuration > Network Devices**.
- b) Select the device on which you want to configure these changes by clicking the device name hyperlink.

- c) Click the **Configuration** tab and choose **Routing > OSPF**.
- d) Select the required process by clicking the process ID hyperlink.
- e) Click the **OSPF Interfaces** tab.
- f) Click the Add ('+') icon to add new settings to the interfaces associated with the selected device's OSPF process. To edit existing values, click the Interface Name hyperlink and click the Edit icon at the top right of the page.
- g) Specify the parameters as explained in the table below.
- h) Click **Save** to deploy your changes to the device.

Option	Description
<b>OSPF Common Properties</b>	<b>Description</b>
Process ID	Unique numerical value between 1 and 65535 that identifies the selected OSPF process.
Router ID	Router ID of the Area 0 router.
Cost	Sets a cost for sending packets across the network, which is used by OSPF routers to calculate the shortest path. This is not enabled for Cisco IOS-XE devices. Enter a numeric value between 1 and 65535.
Topology Priority	Displays the designated router for a subnet. Enter a numeric value between 1 and 255.
Maximum number of paths per route	Defines the highest number of paths that can be used by the router for load balancing per route. The default value is 4. You can set a numeric value between 1 and 64.
Administrative Distance	Specifies the distance that will be set for path selection. The default value is 110 and the available values are between 1 and 255.
External Area Distance	Specify the distance for external type 5 and type 7 routes. Your options are any numeric value between 1 and 255.
Inter Area Distance	Specify the inter area distance for inter-area routes using a value between 1 and 255.
Intra Area Distance	Specify the intra area distance for intra-area routes using a value between 1 and 255.
<b>Routing &gt; OSPF &gt; OSPF Interface/PEP Properties</b>	<b>Description</b>
Area ID	Specify the OSPF area ID for the NEs using an integer between the 0 and 4294967295. The ID cannot be 0.0.0.0.
Interface Name	Device's interface with which the specified OSPF interface/pep settings must be associated.
Interface cost	Cost of sending packets across the network. This cost is used by OSPF routers to calculate the shortest path.
Interface Priority	Designated router for a subnet.
Network Type	Type of network associated with the OSPF process. Your options are: Broadcast, NBMA, Point to Point, and Point to Multipoint.

Option	Description
Dead Interval	Number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. The Cisco default is 40 seconds.
Hello Interval	Number of seconds between OSPF hello packet advertisements sent by OSPF routers. The Cisco default is 10 seconds.
Retransmit Interval	Time that will elapse before a packet is resent. The Cisco default is 5 seconds.
Transmit Delay	Service speed. The Cisco default is 1 second.

## Configure RIP

Routing Information Protocol (RIP) is a distance-vector routing protocol that uses hop count as a routing metric. RIP implements a limit of 15 hops in a path from source to a destination, to prevent routing loops. The hop-count limit also limits the size of the networks that RIP supports. RIP sends its routing table every 30 seconds.

The variants of RIP are RIP version 1 (described in RFC1058) and RIP version 2 (described in RFC2453). RIP uses the split horizon, route poisoning, and holddown mechanisms to prevent incorrect routing information from being propagated.

- 
- Step 1** Choose **Configuration > Network Devices**.
- Step 2** Click the device hyperlink to launch its Device Details page.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **Routing > RIP**. The RIP Routing page appears with options to configure IPv4 and IPv6 (depending on the device you select) RIP routes.
- Step 5** Expand the **IPv4 RIP Routes** and **IPv6 RIP Routes** drop-down menus to specify the following RIP parameters.
- Note** You can specify the IPv6 addresses depending on your device selection. For example, for Cisco IOS-XR devices, you can only specify IPv4 RIP routes.
- Select the RIP version.
  - Expand the **IPv4 RIP Routes** drop-down, click the Add (+) button, and enter the IPv4 addresses that must be included for the selected RIP version. A valid IP address consists of 4 octets separated by '!'. Each octet must be in the range 0-255. The only valid IPv4 address starting with 0 is 0.0.0.0.
  - Use the **Passive Interface** tab to select the loopback0 or tunnel values that must be associated as passive interfaces with the RIP route. Depending on the type of device you select, this tab may be hidden. For example, for Cisco IOS-XR devices, you cannot specify passive interfaces.
  - Expand the **IPv6 RIP Routes** drop-down, click the Add (+) button to enter the IPv6 addresses. Depending on the type of device you select, this drop-down may be hidden. For example, for Cisco IOS-XR devices, you cannot specify IPv6 addresses.
  - Click **Save** to deploy your changes to the device.
-

## Configure Static Routing

Static routing is the simplest form of routing, where the network administrator manually enters routes into a routing table. The route does not change until the network administrator changes it. Static routing is normally used when there are very few devices to be configured and the administrator is very sure that the routes do not change. The main drawback of static routing is that a change in the network topology or a failure in the external network cannot be handled, because routes that are configured manually must be updated to fix any lost connectivity.

---

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

**Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.

**Step 4** Choose **Routing > Static**.

**Step 5** To configure static routing, click **Add**.

- a) In the Basic Configuration area, at a minimum, enter the Interface Number (if not already populated). You can also enter a description, MTU (in bytes), and bandwidth (in Kbps).
- b) If you are creating an IPv4 VLAN interface, select an IP Type:
  - Static, with the IP address and subnet mask
  - DHCP IP, with the pool name

You can also enter a secondary IP address with mask.

- c) If you are adding an IPv6 VLAN interface, in the IPv6 Address area, select a type from the Add drop-down list: Global, Unnumbered, Link Local, Auto Configuration, or DHCP.
  - Global, with the IP address and subnet mask, and type (General, EUI-64, Anycast, CGA)
  - Unnumbered, and enter text in the Interface Unnumbered To text box
  - Link Local, auto-configured or manually-configured (requires IPv6 address)
  - Autoconfiguration
  - DHCP (with option to enable two-message exchange for address allocation)

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

---

## Configure ACLs

The Configuration tab in the Device Details page lists the current CFM configuration on the device. Depending on your device configuration and user account privileges, you can configure ACLs on the device.

To configure ACLs:

---

**Step 1** Choose **Configuration > Network Devices**.

**Step 2** Click the device hyperlink to launch its Device Details page.

- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **Security > ACL**.
- Step 5** Specify the following parameters for the ACL:
- a) Name/Number- Specify a unique identifier for the ACL. You can use alphanumeric characters, hyphens, and underscores.
  - b) Type- Specify whether the ACL is of type standard or extended. This drop-down menu is hidden depending on the type of device you select. For example, for Cisco IOS-XR devices this drop-down menu is hidden.
  - c) (Optional) Description- Enter a description about the ACL for reference.
- Step 6** Click **Save** to save your values in the Cisco EPN Manager . This does not deploy your changes to the device.
- Step 7** Click the drop-down icon next to the ACL created in the above steps and specify the following ACE values:
- a) Click **Add Row** to add a new ACE or select an existing ACE and click **Edit**, to specify the Action (Permit or Deny), Source IP, and optionally the wild card source and description that must be associated with the ACE.
  - b) Click **Save** to save the values associated with the ACE.
  - c) Use the up and down arrows (buttons) to specify the order in which the ACEs must be applied on the device for the selected ACL.
- Step 8** Select the ACL created in the above steps and click **Apply to Interface** to specify the interface(s) on which this ACL must be applied.
- Step 9** Click **OK** to deploy the specified ACL values to the selected interfaces of the device.
- 

## Configure EOAM Fault and Performance Monitoring

Cisco EPN Manager enables you to prepare the devices in your network for using EOAM (Ethernet Operations, Administration and Management) protocol for monitoring and troubleshooting Carrier Ethernet services. You can configure Connectivity Fault Management (CFM) on the devices participating in the Ethernet services. You can also perform connectivity and performance tests on the Ethernet services using sets of CLI commands available as predefined templates in Cisco EPN Manager.

### Configure CFM

Cisco EPN Manager allows you to configure CFM domains, services, and maintenance endpoints on devices in your network. This CFM configuration sets the stage for using the EOAM protocol to monitor and troubleshoot Carrier Ethernet services. CFM must be configured on the endpoints of the service. This can be done per device using the procedure described in [Configure CFM Maintenance Domains and Maintenance Associations \(Services\)](#), on page 364. Alternatively, CFM can be configured on the EVC level when creating and provisioning an EVC, as described in [Create and Provision a New Carrier Ethernet EVC](#), on page 437.

Once CFM is configured, you can quickly and easily view the CFM settings on individual devices and make changes if necessary. For example, if there is a problem with traffic flow across a specific EVC, you might want to make the continuity check interval shorter temporarily in order to analyze the problem, keeping in mind that this will increase the management traffic and thus might impact network performance. You can change the setting on the specific device rather than re-provisioning the entire service.

See these topics for more information:

- [CFM Overview](#), on page 363
- [Configure CFM Maintenance Domains and Maintenance Associations \(Services\)](#), on page 364



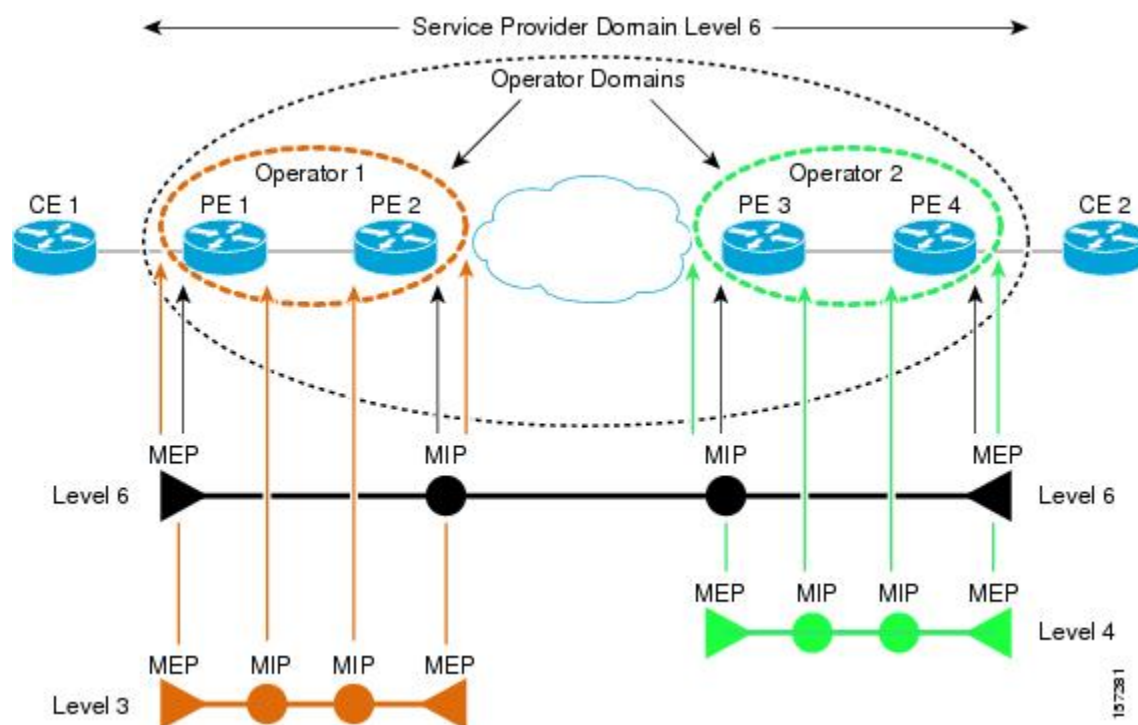
## CFM Overview

IEEE Connectivity Fault Management (CFM) is an end-to-end per-service Ethernet layer Operations, Administration, and Maintenance (OAM) protocol. CFM includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

CFM operates on a per-Service-VLAN (or per-EVC) basis. It lets you know if an EVC has failed, and if so, provides the tools to rapidly isolate the failure.

A CFM-enabled network is made up of maintenance domains, CFM services and maintenance points, as described below.

**Figure 2: CFM Maintenance Domains**



### Maintenance Domains

Ethernet CFM, within any given service provider network, relies on a functional model consisting of hierarchical maintenance domains. A maintenance domain is a management space on a network that is owned and operated by a single entity and defined by a set of internal boundary ports. A domain is assigned a unique maintenance level which defines the hierarchical relationship of domains. Maintenance domains may nest or touch, but cannot intersect. If two domains nest, the outer domain must have a higher maintenance level than the one it engulfs. A single device might participate in multiple maintenance domains.

### CFM Services

A CFM service (maintenance association) enables the partitioning of a CFM maintenance domain according to the connectivity within the network. For example, if the network is divided into a number of virtual LANs (VLANs), a CFM service is created for each of these. CFM can then operate independently in each service. A CFM service is always associated with the maintenance domain within which it operates, and therefore with that domain's maintenance level. All CFM frames relating to the service carry the maintenance level of

the associated maintenance domain. There can be many CFM services within a domain. The CFM service must be configured on a domain before MEPs can be configured.

### Maintenance Points

A maintenance point demarcates an interface that participates in a CFM maintenance domain. A maintenance point is an instance of a particular CFM service on a specific interface. CFM only operates on an interface if there is a CFM maintenance point on the interface. A maintenance point is always associated with a particular CFM service, and therefore with a particular maintenance domain at a particular level. Maintenance points generally only process CFM frames at the same level as their associated maintenance domain. Frames at a higher maintenance level are always forwarded transparently, while frames at a lower maintenance level are normally dropped. This helps enforce the maintenance domain hierarchy and ensures that CFM frames for a particular domain cannot leak out beyond the boundary of the domain. There are two types of maintenance points:

- **Maintenance endpoints (MEPs)**—Created at the edge of the domain. Responsible for confining CFM messages within the domain. Maintenance end points (MEPs) are members of a particular service within a domain and are responsible for sourcing and sinking CFM frames. They periodically transmit continuity check messages and receive similar messages from other MEPs within their domain. They also transmit traceroute and loopback messages at the request of the administrator.
- **Maintenance intermediate points (MIPs)**—Internal to the domain. A MIP will forward CFM packets while MEPs do not forward CFM packets because they must keep them within the domain. MIPs are not explicitly configured on each interface. MIPs are created automatically according to the algorithm specified in the CFM 802.1ag standard.

## Configure CFM Maintenance Domains and Maintenance Associations (Services)

To enable CFM in your network, you need to create the relevant maintenance domains and define the maintenance points participating in the maintenance domain. For each device, you specify to which maintenance domain it belongs by assigning a maintenance domain level. You then define the CFM services, where you associate MEPs with the maintenance domain, that is, the interfaces on the device that belong to the maintenance domain.

To configure CFM on a device:

### Before you begin

If you want to associate MEP parameters while configuring CFM, ensure that the following commands have been configured on the devices:

#### For Cisco IOS and Cisco IOS-XE devices:

```
interface <type of interface, gigabit/tengigabit> <interface number>
  service instance <service instance number, for example 1> ethernet
  encapsulation dot1q 1 <vlan id>
```

- 
- Step 1** Choose **Inventory > Network Devices** from the left sidebar.
  - Step 2** Locate the required device in the list of devices and click the device name hyperlink to open the device details window.
  - Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
  - Step 4** Choose **EOAM > CFM**.
  - Step 5** In the CFM window, click the '+' icon to add a new CFM domain.

- Step 6** Enter the following information:
- **Maintenance Domain Name**—Enter the name of the maintenance domain to which the device belongs.
  - **MEP Archive Hold Time**—Enter the number of minutes that data from a missing maintenance end point (MEP) is kept before it is purged. The range is 1 to 65535.
  - **Level**— Select a maintenance level (0 to 7) from the **Level** drop-down menu. The level defines the maintenance domain to which the device belongs. A device might belong to more than one maintenance domain, in which case it would be assigned to more than one maintenance level.
- Step 7** Click **Save**. The row is added to the table and the configurations are deployed to the device. Now you can define the CFM services and associate end points to the configured maintenance domain. Once the configuration is deployed to the device, you can edit only the MEP Archive Hold Time value in the row. The other values cannot be modified.
- Step 8** Locate the maintenance domain name you just created in the table and click on the Maintenance Domain name hyperlink.
- Step 9** Click the **Services** tab to add service details.
- Step 10** Enter a name for the CFM service.
- Step 11** For IOS devices: Enter a bridge domain name.  
For IOS-XR devices: Enter the X-connect group name and the name of the point to point connection within the cross connect group.
- Step 12** Change the interval (10 to 600000 ms) between messages using the **Continuity Check Interval** drop-down menu.
- Step 13** Locate the CFM service you just created in the table and click on the MEP hyperlink. This link was enabled when you saved the details.
- Step 14** In the **MEP** tab, specify the interfaces that will serve as the MEPs in the Maintenance Entity Group. These are the interfaces on the device that belong to the specified maintenance domain, have the same level, and are on the same service provider VLAN (S-VLAN).  
If the **Interface** drop-down menu is empty, ensure that the device is configured with the pre-requisites mentioned above.
- Step 15** For each MEP, enter the MEP ID (a value between 1 and 8191).
- Step 16** Click **Save** to save your MEP definitions and close the dialog. To verify that your changes were saved, navigate to **Inventory > Network Devices**, and in the Configuration tab, click **EOAM > CFM** and view the maintenance domain details.

### Delete a CFM Domain

You can delete CFM domains that have been created using Cisco EPN Manager. To delete a CFM domain:

- Step 1** Choose **Inventory > Network Devices** from the left sidebar.
- Step 2** Locate the required device in the list of devices and click the device name hyperlink to open the device details window.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Choose **EOAM > CFM**.
- Step 5** Select the domain that you want to delete and in the CFM window, click the 'X' icon to delete it. This deletes the configured maintenance domain both from the table and from the device. If the domain has defined CFM services and associated end points, then you will need to disassociate the services and the end points before deleting the domain.

## Perform EOAM Connectivity and Performance Checks

Cisco EPN Manager provides predefined EOAM-related configuration templates that can be used to monitor the connectivity and performance of virtual connections (VCs) in a Carrier Ethernet network.

To use these templates, from the left sidebar, choose **Configuration > Templates > Features & Technologies**, then choose **CLI Templates > System Templates – CLI**.

The following table lists the available EOAM configuration templates, their purpose, and the mandatory input parameters you are required to provide.


**Note**

To see the results and/or output of template deployment, check the job details that are displayed when you deploy a change.

**Table 24: EOAM Templates**

Template Name	Use it to...	Essential Input Values	Additional Information
EOAM-CCDB-Content-IOS	Display the contents of a maintenance intermediate point (MIP) continuity check database (CCDB) in order to verify CFM operation or to check how EOAM has been set up in the network.	None of the fields are mandatory.  <b>Domain ID:</b> Choose the way in which you want to identify the maintenance domain and enter a value in the corresponding field.  <b>Service:</b> Specify a maintenance association within the domain, based on ICC MEG identifier, VLAN ID or VPN ID.	
EOAM-CCDB-Content-IOS-XR	Display the contents of a maintenance intermediate point (MIP) continuity check database (CCDB) in order to verify CFM operation or to check how EOAM has been set up in the network.	None of the fields are mandatory.  <b>Node ID:</b> The CFM CCM learning database for the designated node, entered in the rack/slot/module notation.	
EOAM-CFM-Ping-IOS and EOAM-CFM-Ping-IOS-XR	Check connectivity to a destination MIP or MEP using CFM loopback messages.	<b>Ping Destination Type:</b> Identify the destination MEP, either by MAC address or MEP ID. Choose Multicast if there are multiple destination MEPs.  Maintenance domain name for destination MEP: The name of the domain where the destination MEP resides.	

Template Name	Use it to...	Essential Input Values	Additional Information
EOAM-CFM-Traceroute- IOS	IOS devices: Trace the route to a destination MEP to check the number of hops and the connectivity between hops.	<p><b>Destination Type:</b> Identify the destination MEP, either by MAC address or MEP ID.</p> <p><b>Maintenance domain name for destination MEP:</b> The name of the domain where the destination MEP resides.</p> <p><b>Service Type:</b> Identify the maintenance association (MA) within the domain, either by name, ITU carrier code (ICC), MA number, VLAN ID, or VPN ID.</p>	
EOAM-CFM-Traceroute- IOS-XR	IOS-XR devices: Trace the route to a destination MEP to check the number of hops and the connectivity between hops.	<p><b>Maintenance domain name for destination MEP:</b> The name of the domain where the destination MEP resides.</p> <p><b>Service Name:</b> The name of the service instance being monitored by the Maintenance Association (MA) within the specified maintenance domain.</p> <p><b>Destination Type:</b> Identify the destination MEP, either by MAC address or MEP ID.</p> <p><b>Source MEP ID:</b> Identify the maintenance association (MA) within the domain, either by name, ITU carrier code (ICC), MA number, VLAN ID, or VPN ID.</p> <p><b>Source Interface Type:</b> The source interface type of the locally defined CFM MEP.</p> <p><b>Interface Path ID:</b> The physical or virtual interface name.</p>	
EOAM-Configure-Y- 1731-PM-On-Demand- Operation-CFM-Loopback- IOS-XR	Configure an on-demand Ethernet SLA operation for CFM loopback. By default, measures two-way delay and jitter.	<p><b>Probe Domain:</b> Check the checkbox to enable the probe.</p> <p><b>Domain Name:</b> The name of the maintenance domain for the locally defined CFM MEP.</p> <p><b>Domain Interface Type:</b> The source interface type of the locally defined CFM MEP.</p> <p><b>Domain Interface Path ID:</b> The physical or virtual interface name.</p> <p><b>Domain MAC Address or MEP-ID:</b> Choose whether you want to identify the domain by MAC address or by MEP ID and provide the necessary information in the relevant field below. For MEP ID, enter an ID from 1 to 8191.</p>	Optionally, you can specify the type of statistics to measure, whether or not to use bins for aggregate type, probe frequency and duration values, and more. The values you specify will override the default actions.

Template Name	Use it to...	Essential Input Values	Additional Information
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Synthetic-Loss-Measurement-IOS-XR	Configure an on-demand Ethernet SLA operation for CFM synthetic loss measurement. By default, measures one-way Frame Loss Ratio (FLR) in both directions.	<p><b>Probe Domain:</b> Check the checkbox to enable the probe.</p> <p><b>Domain Name:</b> The name of the maintenance domain for the locally defined CFM MEP.</p> <p><b>Domain Interface Type:</b> The source interface type of the locally defined CFM MEP.</p> <p><b>Domain Interface Path ID:</b> The physical or virtual interface name.</p> <p><b>Domain MAC Address or MEP-ID:</b> Choose whether you want to identify the domain by MAC address or by MEP ID and provide the necessary information in the relevant field below. For MEP ID, enter an ID from 1 to 8191.</p>	Optionally, you can specify the type of statistics to measure, whether or not to use bins for aggregate type, probe frequency and duration values, and more. The values you specify will override the default actions.
EOAM-Configure-Y-1731-PM-On-Demand-Operation-FM-Delay-Measurement-IOS-XR	Configure an on-demand Ethernet SLA operation for CFM delay measurement. By default, measures one-way delay and jitter in both directions, and two-way delay and jitter.	<p><b>Probe Domain:</b> Check the checkbox to enable the probe.</p> <p><b>Domain Name:</b> The name of the maintenance domain for the locally defined CFM MEP.</p> <p><b>Domain Interface Type:</b> The source interface type of the locally defined CFM MEP.</p> <p><b>Domain Interface Path ID:</b> The physical or virtual interface name.</p> <p><b>Domain MAC Address or MEP-ID:</b> Choose whether you want to identify the domain by MAC address or by MEP ID and provide the necessary information in the relevant field below. For MEP ID, enter an ID from 1 to 8191.</p>	Optionally, you can specify the type of statistics to measure, whether or not to use bins for aggregate type, probe frequency and duration values, and more. The values you specify will override the default actions.

Template Name	Use it to...	Essential Input Values	Additional Information
EOAM-Configure-Y-1731-PM-Direct-On-Demand-IOS	Perform real-time troubleshooting of Ethernet services in direct mode where an operation is created and run immediately.	<p>Frame Type: The type of frame, either DMMv1 (frame delay) or SLM (frame loss).</p> <p>Domain Name: The name of the maintenance domain for the locally defined CFM MEP.</p> <p>EVC or VLAN: Identify the EVC or VLAN on which the test will be performed. The VLAN ID can be between 1 and 4096.</p> <p>Target MPID or MAC Address: Identify the MEP at the destination, either by MPID (1 to 8191) or by MAC Address.</p> <p>CoS Value: The class of service level (0-7) that will be applied to the CFM message for the specified MEP.</p> <p>Local MPID or MAC Address: Identify the MEP at the source, either by MPID (1 to 8191) or by MAC Address.</p> <p>Burst or Continuous: Specify whether a continuous stream of frames or bursts of frames will be sent during the on-demand operation.</p> <p>Aggregation Period: Specify the length of time in seconds during which the performance measurements are conducted, after which the statistics are generated (1-900).</p>	
EOAM-Configure-Y-1731-PM-Referenced-On-Demand-IOS	Perform real-time troubleshooting of Ethernet services in referenced mode where a previously configured operation is started and run.	<p>Frame Type: The type of probe, either DMMv1 or SLM.</p> <p>Operation Number: The number of the operation being referenced.</p>	
Remove-CFM-MEP-IOS	Remove the MEP configuration from the device.	Interface Name, Service Instance Number, EVC Name.	
Remove-CFM-MEP-IOSXR	Remove the MEP configuration from the device.	Interface Name, Domain Name.	
Remove-CFM-Service-IOS	Remove the CFM service.	Interface Name, Service Instance Number, EVC Name, Domain Name, Level, Service Name.	

## Configure Quality of Service (QoS)

Quality of Service (QoS) is a set of capabilities that allow the delivery of differentiated services for network traffic. QoS features provide better and more predictable network service by:

- Giving preferential treatment to different classes of network traffic.
- Supporting dedicated bandwidth for critical users and applications.
- Controlling jitter and latency (required by real-time traffic).
- Avoiding and managing network congestion.
- Shaping network traffic to smooth the traffic flow.
- Setting traffic priorities across the network.

Using Cisco EPN Manager you can configure QoS on Carrier Ethernet interfaces. Before the appropriate QoS actions can be applied, the relevant traffic must be differentiated by creating classification profiles, or class maps. Packets arriving at the device are checked against the match criteria of the classification profile to determine if the packet belongs to that class. Matching traffic is subjected to the actions defined in an action profile, or policy map.

To configure classification profiles and action profiles, choose **Configuration > QoS > Profiles** from the left sidebar.

This section includes the following topics:

- [Create a QoS Classification Profile, on page 370](#)
- [Create a QoS Action Profile, on page 372](#)
- [Check Which QoS Profiles are Configured on a Device, on page 377](#)
- [Apply a QoS Action Profile to Interface\(s\), on page 378](#)
- [Import QoS Profiles Discovered from Devices, on page 378](#)
- [Dissociate a QoS Action Profile from Multiple Interfaces, on page 379](#)
- [Delete QoS Classification and Action Profiles from Devices, on page 380](#)

## Create a QoS Classification Profile

Create classification profiles (class maps) to differentiate traffic into different classes so that certain actions can be applied to traffic that matches the classification criteria.

To create a classification profile:

- 
- Step 1** Choose **Configuration > QoS > Profiles** in the left sidebar.
- Step 2** Click the Add (“+”) icon at the top of the Global QoS Classification Profiles pane.
- Step 3** Enter a unique name for the classification profile. The name should reflect the classification criteria defined in the profile for easy identification. For further clarification, you can add a description.
- Step 4** Define the matching criteria for the profile:
- Match All—All the classification criteria must be met in order for the traffic to belong to this class.
  - Match Any—Any of the classification criteria can be met in order for the traffic to belong to this class.
- Step 5** Under QoS Classifications, click the plus icon to define classification criteria for the classification profile.



**Step 6**

Select an action based on which the traffic will be classified, then click in the Value column and provide the relevant value, as follows:

Action	Description	Value
ACL	The packet must be permitted by the specified access control list (ACL).	The name of the ACL. A string of up to 32 alphanumeric characters.
MPLS - Imposition	The experimental (EXP) bit value on the imposed label entry of the packet must match the MPLS EXP value that you specify. Use either the MPLS Imposition or the MPLS Topmost for matching criteria. Once you have used one of the MPLS criteria, the other one will no longer be available.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
MPLS - Topmost	The experimental (EXP) bit value in the topmost label must match the MPLS EXP value that you specify.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
Cascade	This action is used to cascade one class map into another. It can be used when creating a new class map which has classification policies similar to an existing class map.	Reference the child class map.
QoSClassification - COS	The packet's layer 2 class of service (CoS) bit value must match the specified CoS value.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
QoSClassification - COS - Inner	The specified value must match packet's inner CoS value of QinQ packets for Layer 2 class of service (CoS) marking.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
QoSClassification - DSCP	The packet IP differentiated service code point (DSCP) value must match one or more of the specified values.	Valid values are from 0 to 63. Up to 8 comma-separated values can be entered.
QoSClassification - DSCP - IPv4 only	Match DSCP values for IPv4 packets.	Valid values are from 0 to 63. Up to 8 comma-separated values can be entered.
QoSClassification - Precedence	The packet IP precedence value must match one or more precedence values.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
QoSClassification - Precedence - IPv4 only	Match precedence values for IPv4 packets.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
QoSClassification - DEI	Drop eligible indicator (DEI) is used to indicate frames eligible to be dropped when there is congestion. The packet must match the DEI value specified.	0 or 1.
QoS-Group	The packets must be permitted based on the selected QoS group.	Up to 8 comma separated unique values ranging from 0-55 or 0-99 based on the selected device. Ensure that the value you enter is supported on the device.

Action	Description	Value
QoSClassification - Service Instance	Service Provider configurations have various service instances on the Provider Edge (PE) routers. QoS policy-maps are applied on these service instances or group of service instances.  <b>Note</b> This criteria is applicable only on Cisco ASR 903.	Accepts any number of comma separated values ranging from 1-4000 and/or hyphenated value with each ranging from 1-4000.
QoSClassification - Discard Class	Indicates that packets must be permitted/discarded based on the selected discard class.	Accepted value is any number between 0-7.
QoSClassification - Traffic Class	Traffic class of the QoS configuration.	Accepted value is any number between 0-7.

**Step 7** Define additional QoS classifications, as required.

**Step 8** Click the **Save** button at the bottom of the window to save the profile. A notification in the bottom right corner will confirm that the profile has been saved and the profile will appear in the list of profiles on the left.

**Step 9** Select the profile from the list and click the **Deploy** button to initiate deployment of the profile to devices.

**Step 10** If you want to create a new profile with the details of an existing Classification Profile, click the **Clone** button. This profile will have the name of the classification profile that you cloned from, and the suffix **-clone**. You can edit the name, matching criteria and any other details of this cloned profile.

**Step 11** If you want the selected profile to override any other class map that already exists on the device, check the **Override existing configuration** check box. If this check box is not checked, the profile will be merged with the configurations on the device.

**Step 12** Select the device(s) to which you want to deploy the QoS Classification profile.

**Step 13** Schedule the deployment, if required.

**Step 14** Click **Submit**. A notification in the bottom right corner will confirm that the profile has been deployed. To check the status of the deployment job, choose **Administration > Job Dashboard** from the left sidebar. Select the relevant job to view the job details and history in the lower section of the window. Click the Information icon for further details.

## Create a QoS Action Profile

Create action profiles (policy maps) to specify the actions to be applied to traffic belonging to a specific traffic class.

To create an action profile:

**Step 1** Choose **Configuration > QoS > Profiles** from the left sidebar.

**Step 2** From the QoS Profiles pane on the left, choose, **User Defined Global QoS Profiles > Action Profiles**.

**Step 3** Click the Add (“+”) icon at the top of the Create Action Profile pane

**Step 4** Enter a unique name for the action profile, and enter a description, if required.

**Step 5** Select the classification profiles for which you want to assign actions. Under Classification Profiles, click the plus icon, select the required profile(s) from the list, and click **OK**.

**Step 6**

Select the Classification Profile (class map) and define the actions to be applied if traffic matches the profile. You can define Policing, Marking, Queuing, Shaping, RED actions, and Service Policy (H-QoS). There is a tab for each of these action types and its definitions, as follows:

- **Policer Action:** Traffic policing manages the maximum rate of traffic allowed on an interface through a token bucket algorithm. Traffic policing also provides a certain amount of bandwidth management by allowing you to set the burst size (Bc) for the CIR. When the peak information rate (PIR) is supported, a second token bucket is enforced and this two-rate policer can meter traffic at two independent rates: the committed information rate (CIR) and the peak information rate (PIR). The committed token bucket can hold bytes up to the size of the committed burst (bc) before overflowing and determines whether a packet conforms to or exceeds the CIR. The peak token bucket can hold bytes up to the size of the peak burst (Be) before overflowing, and determines whether a packet violates the PIR. Different actions can be taken if a packet conforms, exceeds, or violates the CIR/PIR. For instance, packets that conform can be configured to be sent, packets that exceed can be configured to be sent with a decreased priority, and packets that violate can be configured to be dropped.

In the Policer Action tab, specify the following:

- **Committed Information Rate (CIR)**—The long-term average transmission rate, specified in bits per second (bps) or as a percentage of the available or unused bandwidth. Traffic that falls under this rate will always conform. Ensure that the CIR value you enter is supported on the device and choose the right CIR unit value (bps, kbps, mbps, gbps, or percent).
- **Burst (Bc)**—How large traffic bursts can be (in bytes) before some traffic exceeds the CIR.
- **Peak Information Rate (PIR)**—How much traffic bursts can peak before some traffic exceeds the PIR value associated with the CIR. Ensure that the PIR value you enter is supported on the device and choose the same unit value you chose for CIR (bps, kbps, mbps, gbps, or percent).
- **Excess Burst (Be)**—How large traffic bursts can be (in bytes) before traffic exceeds the PIR.
- **Under Traffic Coloring Behaviour**, select the action to be performed if the traffic conforms, exceeds, or violates the rate limit. Provide values as required. To enable color-aware traffic policing specify the Conform Color and Exceed Color values by associating them with respective class profiles. With color-aware policing, the following results occur based on the CIR, the PIR, and the conform actions, exceed actions, and violate actions:
  - Packets that have metering rates less than or equal to the CIR and belong to the specified class (conform-color) are policed as conforming to the rate. These packets are also policed according to the conform action specified. In this instance, the packets will be transmitted.
  - Packets that have metering rates between the CIR and the PIR and belong to either to the conform-color class or exceed-color class are policed as exceeding the CIR. These packets are also policed according to the exceed action specified. In this instance, the precedence value of the packets will be set and the packets transmitted.
  - Packets that have metering rates higher than the PIR or belong to neither class conform-color or class exceed-color are policed as violating the rate. These packets are also policed according to the violate action specified. In this instance, the packets will be dropped.
- **Marker Action:** Packet marking allows you to partition your network into multiple priority levels or classes of service. Marking of a traffic flow is performed by:
  - Setting IP Precedence or DSCP bits in the IP Type of Service (ToS) byte .
  - Setting CoS bits in the Layer 2 headers.

- Setting EXP bits within the imposed or the topmost Multiprotocol Label Switching (MPLS) label.
- Setting qos-group, traffic-class, and discard-class bits.

In the Marker Action tab, specify the following:

- **Marking Feature and Marking Value**—The method by which the traffic will be marked, and the required value.
- **Queueing Action:** Queueing is used for traffic congestion management. It entails the creation of queues, assignment of packets to those queues based on the classification of the packet, and scheduling of the packets in a queue for transmission.

In the Queueing Action tab, select the method by which traffic will be queued, either Bandwidth or Priority, then specify the following:

- **Bandwidth**—The amount of bandwidth to be assigned to the traffic class, either in kilobits per second, or as a percentage of absolute guaranteed bandwidth. If you selected to queue by bandwidth, you can also assign bandwidth as a percentage of remaining bandwidth.
- **Queue Limit**—The maximum number of packets/bytes/milliseconds for all the individual queues associated with this class. When the queue size exceeds this value, packets will be dropped.

If you selected Bandwidth, specify the following:

- **Enable Fair Queue**—Check the check box to enable weighted fair queueing.
- **Individual Queue Size**—Relevant if fair queueing is enabled. Specify the maximum number of packets allowed in each per-class queue during periods of congestion.

If you selected Priority, specify the following:

- **Queue Burst Size (bytes)**—The burst size configures the network to accommodate temporary bursts of traffic. Range is 18 to 2000000 bytes. Default is 200 milliseconds of traffic at the configured bandwidth rate.
- **Priority Level**—Classes under a policy map can have different priority, from priority queue level 1 to 3. Packets on these queues are subjected to less latency with respect to other queues. You cannot specify the same priority level for two different classes in the same policy map.
- **Shaping Action:** Traffic shaping regulates traffic by shaping it to a specified rate.

In the Shaping Action tab, specify the following:

- **Select Average or Peak rate traffic shaping**—Average rate shaping limits the transmission rate to the CIR. Peak rate shaping configures the router to send more traffic than the CIR. To determine the peak rate, the router uses the following formula:  $\text{peak rate} = \text{CIR}(1 + \text{Be} / \text{Bc})$  where Be is the Excess Burst size and Bc is the Committed Burst size.
- If you selected Peak rate traffic shaping, specify the burst size and the excess burst size in bytes.
- If required, enable FECN Adaptive Shaping. Adaptive shaping estimates the available bandwidth when backward explicit congestion notification (BECN) signals are received. With FECN adaptive shaping, the router reflects forward explicit congestion notification (FECN) signals as BECN signals.
- If FECN Adaptive Shaping is enabled, specify the Adaptive Rate, which is the minimum bit rate to which the traffic is shaped.

- **RED Action:** Weighted Random Early Detection (WRED) is a congestion avoidance technique that implements a proactive queuing strategy that controls congestion before a queue reaches its queue limit. WRED combines the capabilities of the random early detection (RED) mechanism with IP precedence, differential services code point (DSCP), and discard-class to provide preferential handling of higher priority packets. When an interface starts to become congested, WRED discards lower priority traffic with a higher probability. WRED controls the average depth of Layer 3 queues.

In the RED Action tab, specify the following:

- **Classification Mechanism**—Select the basis upon which the WRED drop policies are defined. For WRED, you define drop policies based on specific packet classification, as follows:
  - CLP**—Configures a drop policy for WRED based on a cell loss priority (CLP) value. Valid values are 0 or 1.
  - CoS**—Configures a drop policy for WRED based on the specified class of service (CoS) bit associated with the packet. Valid values are from 0 to 7.
  - Discard Class**—Configures a drop policy for WRED based on a discard-class value. Valid values are from 0 to 7. The discard-class value sets the per-hop behavior (PHB) for dropping traffic. WRED based on discard-class is an egress function.
  - DSCP**—Configures a drop policy for WRED based on a DSCP value. When configured, the router randomly drops packets with the specified DSCP value, according to the WRED thresholds you configure.
  - Precedence**—Configures a drop policy for WRED based on an IP precedence level. Valid values are from 0 to 7, where 0 typically represents low priority traffic that can be aggressively managed (dropped) and 7 represents high priority traffic. Traffic at a low precedence level typically has a higher drop probability. When WRED drops packets, source hosts using TCP detect the drops and slow the transmission of packets.
  - DEI**—The discard eligibility (DE) bit in the address field of a frame relay frame is used to prioritize the discarding of frames in congested frame relay networks. The frame relay DE bit has only one bit and therefore only has two settings, 0 or 1. If congestion occurs in a frame relay network, frames with the DE bit set at 1 are discarded before frames with the DE bit set at 0.
  - RED Default**—The default set of minimum thresholds, maximum thresholds, and Mark Probability Denominator (MPD) settings for a class in the WRED profile.
- If required, enable ECN. ECN (Explicit Congestion Notification) marks packets instead of dropping them when the average queue length exceeds a specific threshold value. Routers and end hosts use this marking as a signal that the network is congested and slow down packet transmission.
- Define the thresholds and mark probability per valid value of the selected classification mechanism. For example, if you are using Precedence, you can define thresholds for each of the 7 valid values. The minimum threshold is the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops *some* packets with the specified DSCP, IP precedence, discard-class, or atm-clp value. Valid minimum threshold values are from 1 to 16,384. The maximum threshold is the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP, IP precedence, discard-class, or atm-clp value. Valid maximum threshold values are from the value of the minimum threshold to 16,384.

- **Service Policy:**

Using the Service Policy tab, you can configure Hierarchical QoS (H-QoS) which enables you to specify QoS behavior at multiple levels of hierarchy. You can use H-QoS to specify multiple policy maps to shape multiple queues together. All hierarchical policy types consist of a top-level parent policy and one or more child policies. The service-policy command is used to apply a policy to another policy, and a policy to an interface.

To configure H-QoS, navigate to the **Service Policy** tab, select the **Enable** check box, and use the **Service Policy** drop-down menu to select the child service policy. The selected child service policy will be associated to the parent policy map that this action profile belongs to. Note that a child service policy cannot act as a parent policy of the same policy map. For example, if a child service policy called X belongs to a parent policy map Y, then the child policy X cannot contain the service policy map Y.

H-QoS Limitations: On Cisco IOS-XE devices such as Cisco ASR903, Cisco ASR907, Cisco ASR920, and Cisco NCS42XX, the following H-QoS limitations are applicable:

- Parent policy map limitations:
  - A parent policy map can be created only using the 'class-default' class.
  - The parent policy map must contain a class with matching criterion such as an EFP (service instance).
  - The parent policy map must contain a class with matching criterion such as VLANs.
- Child policy map limitations:
  - Child policy maps cannot be created with EFP (service instance) and VLAN as the match-type.

- Step 7** Click the **Save** button at the bottom of the window to save the profile. A notification in the bottom right corner will confirm that the profile has been saved and the profile will appear in the list of profiles on the left.
- Step 8** From the Global QoS Action Profiles pane, select the profile, and click the **Deploy** button to initiate deployment of the profile to devices.
- Step 9** If you want to create a new profile with the details of an existing Action Profile, click the **Clone** button. This profile will have the name of the action profile that you cloned from, and the suffix **-clone**. You can edit the name, actions and any other details of this cloned profile.
- Step 10** If you want the selected profile to override any other policy map that already exists on the device, check the **Override existing configuration** check box. If this check box is not checked, the profile will be merged with the configurations on the device.
- Step 11** Select the device(s) to which you want to deploy the QoS Action profile.
- Step 12** Schedule the deployment, if required.
- Step 13** Click **Submit**. A notification in the bottom right corner will confirm that the profile has been deployed. To check the status of the deployment job, choose **Administration > Job Dashboard** from the left sidebar. Select the relevant job to view the job details and history in the lower section of the window. Click the Information icon for further details.

## Create a QoS Sub-Action Profile

An action profile (policy map) specifies the actions to be applied to traffic belonging to a specific traffic class. They are associated with multiple Classification Profiles that define the actions to be applied if traffic matches the profile. You can define Policing, Marking, Queuing, Shaping, RED actions, and Service Policy (H-QoS).

Sub-action profiles are action profiles that are associated with only a single classification profile. You can use sub-action profiles during circuit/VC provisioning to associate a singular action based action profile with the Circuit/VC.

To create a sub-action profile:

- Step 1** Choose **Configuration > QoS > Profiles** from the left sidebar.

- Step 2** From the QoS Profiles pane on the left, choose, **User Defined Global QoS Profiles > Sub-Action Profiles**.
- Step 3** Click the Add (“+”) icon at the top of the Create Sub-Action Profile pane
- Step 4** Enter a unique name for the sub-action profile, and optionally enter a description.
- Step 5** Select the classification profile for which you want to assign actions. Under Classification Profiles, click the plus icon, select the required profile from the list, and click **OK**.
- You can add only a single classification profile to a sub-action profile. To associate multiple classification profiles, you must create an action profile.
- Step 6** Specify the required actions that need to be taken when the traffic matches the criteria specified in the classification profiles. For a description of the various options, see, [Create a QoS Action Profile, on page 372](#).
- 

## Import and Export QoS Action and Sub-Action Profiles

---

- Step 1** Choose **Configuration > QoS > Profiles** from the left sidebar.
- Step 2** To export Action Profiles, choose, **User Defined Global QoS Profiles > Action Profiles** from the pane on the left.
- Step 3** To export Sub-Action Profiles, choose, **User Defined Global QoS Profiles > Sub-Action Profiles** from the pane on the left.
- Step 4** To export profiles, select the profiles that you want to export and click **Export**. The files are saved in the location that you specify.
- Step 5** To import profiles, click **Import**, choose the XML files (that contain information about the action or sub-action profiles) that you want to import, and click **OK**. The imported profiles are listed under the Action Profiles or Sub-Action Profiles pages respectively.

Please note:

- Although there is no limit to the number of profiles you can import in a single instance, we recommend that you choose a maximum of 10 profiles to ensure optimal performance.
  - Ensure that the size of the file you want to import is below 20 MB.
  - Files of only xml format can be imported.
- 

## Check Which QoS Profiles are Configured on a Device

To see the QoS profiles that have been deployed to a specific device:

---

- Step 1** Choose **Inventory > Network Devices** from the left sidebar.
- Step 2** Locate the required device and click on the device name hyperlink to display the device details.
- Step 3** Click the **Configuration** tab, then click the **Logical View** left side tab.
- Step 4** Click on the arrow next to QoS in the left pane, and select either **Action Profiles** or **Classification Profiles**. A table listing the profiles that have been deployed to the selected device is displayed. Click on the profile name (blue hyperlink) to display the details of the profile.
-

## Apply a QoS Action Profile to Interface(s)

You can select an action profile deployed to a device and apply it to multiple interfaces on that device. An action profile enables you to specify the actions to be applied to traffic belonging to a specific traffic class. Before applying an existing profile to interfaces, you can modify the profile or use it to create a new profile. When you choose an interface that has an action profile already applied to it, Cisco EPN Manager notifies you about it and enables you to override the existing profile. To be able to apply an action profile to interfaces, you first need to ensure that the required profile has been deployed to the device. To do this, see [Create a QoS Action Profile, on page 372](#).

To apply an action profile to interfaces:

- 
- Step 1** Choose **Configuration > QoS > Interfaces** from the left sidebar.
- Cisco EPN Manager interfaces are displayed under the categories **Ethernet CSMA/CD**, **IEEE8023 ADLAG**, **Gigabit Ethernet**, and **L2 VLAN**. All other ports are displayed under the **User Defined** category.
- Step 2** Select the interfaces that you want to associate to an Action profile.
- Step 3** Click **Associate Action Profile** to select the action profile and to set the direction in which it must be applied.
- The available action profiles list and the interfaces it can be applied to are listed. The interfaces are listed by their name, application direction, and the action profiles that already exist on the interface.
- Step 4** Select the required action profile from the **Action Profiles** drop-down menu. If the menu is empty, you need to create action profile and then try to associate them with devices. See, [Create a QoS Action Profile, on page 372](#).
- Step 5** In the **Interfaces** section, specify the direction in which the profile is to be applied. While applying a profile to a sub-interface, ensure that it is applied in a direction opposite to that of the main interface. To change the applied direction, use the **Edit** icon at the top left corner of the dialog.
- Note** Policy Maps that contain queuing actions cannot be applied to interfaces in Ingress direction.
- Step 6** (Optional) You can also schedule the application of the selected action profile to a later date and time. To do this, expand the **Schedule** section and specify the date and time and frequency for when you the profile to be applied. This task can further be edited on the Jobs page if required.
- Step 7** Click **OK** to apply the action profile to the selected devices. A notification at the bottom right corner of the dialog will confirm whether the profile has been successfully applied or if the job failed. Click the **Show Details** link for more information.

To dissociate action profiles from the interfaces they are applied to, see [Dissociate a QoS Action Profile from Multiple Interfaces, on page 379](#)

---

## Import QoS Profiles Discovered from Devices

You can import QoS profiles discovered from the device directly into Cisco EPN Manager . Once the QoS profiles are imported, they can be edited and further configured on the device using Cisco EPN Manager . Profiles which are discovered from the device with profile names that match other profiles already present in Cisco EPN Manager are represented as Global profiles. This is indicated in the Global column in the Global Profiles page. Note that Global profiles could have the same names but different QoS configuration. While



importing global profiles, you can choose to either overwrite the existing profile (with the same name) using the discovered profile or you can rename the profile before you import it.

To import QoS profiles discovered from devices:

### Before you begin

Ensure that the device's Inventory Collection status is Completed. This ensures that the QoS profiles from the devices are discovered by Cisco EPN Manager .

- 
- Step 1** Choose **Configuration > QoS > Profiles** from the left sidebar to display all Cisco EPN Manager QoS profiles.
- Step 2** To import Action profiles, from the QoS Profiles pane on the left, choose, **Discovered Profiles > Action Profiles**.
- Step 3** To import Classification profiles, from the QoS Profiles pane on the left, choose, **Discovered Profiles > Classification Profiles**.
- Step 4** To first select a device and choose the profiles discovered on that device:
- Choose **Configuration > Network Devices**, and select the device by clicking the device's Name hyperlink.
  - Click the **Configuration** tab, then click the **Logical View** left side tab.
  - Expand **QoS**.
  - Choose **Action Profiles** or **Classification Profiles** based on the type of profile you want to import from the device.
  - (Optional) After viewing the profiles, to import these profiles directly from the page that lists all QoS profiles discovered by Cisco EPN Manager , click the **Global Profile Page** hyperlink, and skip to Step 5.
  - Select the profiles and click **Make Global**.
  - Go to Step 6.
- Step 5** Select the profiles that you want to import and click **Import**. To ensure that you are importing profiles that are not already present on the device, choose profiles that are not Global (marked as No in the Global column).
- Step 6** If there are duplicate profiles present in Cisco EPN Manager , you are asked to either rename the profile to create a profile with a new name and the same QoS configuration or overwrite the existing profile. Make the required changes.
- Step 7** If you want to create a new profile with the details of an existing QoS Profile , click the **Clone** button. This profile will have the name of the QoS profile that you cloned from, and the suffix **-clone**. You can edit any details of this cloned profile.
- Step 8** Click **Save** to import the selected QoS profiles.
- To apply the imported profiles to a given device's interfaces, see, [Apply a QoS Action Profile to Interface\(s\), on page 378](#).
- 

## Dissociate a QoS Action Profile from Multiple Interfaces

An action profile enables you to specify the actions to be applied to traffic belonging to a specific traffic class. You can select an action profile deployed to a device and apply it to multiple interfaces on that device. After you have applied the profile to the interfaces, you can choose to dissociate them from those interfaces if required. To dissociate an action profile from interfaces, you first need to ensure that the required profile has been applied to the device. See [Apply a QoS Action Profile to Interface\(s\), on page 378](#).

To apply an action profile to interfaces:

- 
- Step 1** Choose **Configuration > QoS > Interfaces** from the left sidebar.

Alternatively, you can navigate to **Configuration > QoS > Profiles** to first select the profile before dissociating it from the interfaces it is applied to.

Cisco EPN Manager interfaces are displayed under the categories **Ethernet CSMA/CD**, **IEEE8023 ADLAG**, and **L2 VLAN**. All other ports are displayed under the **User Defined** category.

- Step 2** Select the interfaces from which you want to dissociate the action profile.
- Step 3** Click **Dis-associate Action Profile**.
- Step 4** (Optional) You can also schedule the de-association of action profiles to a later date and time. To do this, expand the **Schedule** section and specify the date, time, and frequency based on which the profiles must be dissociated.
- Step 5** Click **OK** to confirm. The selected interfaces are dissociated from the action profiles that were applied to them. A notification at the bottom right corner of the window will confirm whether the profile has been successfully dissociated or if the job failed. Click the **Show Details** link for more information.

## Delete QoS Classification and Action Profiles from Devices

To delete QoS classification and action profiles that are deployed to devices, navigate to the paths listed in the table below.



**Note**

You cannot delete QoS action and classification profiles discovered directly from the device. Only profiles created using (and imported into) Cisco EPN Manager can be deleted.

In order to avoid deletion of referenced profiles, the delete operation is not supported in the following scenarios:

- You cannot delete QoS classification profiles associated with other classification profiles. For example if a classification profile uses the Cascade option to reference the selected classification profile, then the delete operation for the selected profile will fail.
- You cannot delete a QoS classification profiles referenced by an action profile.
- Action profiles successfully applied to device interfaces cannot be deleted.
- An action profile cannot be deleted if it is referenced by another action profile. For example, if action profiles are associated to other action profiles by use of a reference policy, then the delete operation of such action profiles fails.

**Table 25: Navigation paths to delete QoS action and classification profiles**

Task	Steps in the GUI
------	------------------

Delete user defined classification profiles	<ol style="list-style-type: none"> <li>1. Choose <b>Configuration &gt; QoS &gt; Classification Profiles</b>.</li> <li>2. Select the classification profile you want to remove from the devices as well as from Cisco EPN Manager .</li> <li>3. Click the <b>X</b> (delete) icon in the task bar.</li> <li>4. Alternatively, you can click the device hyperlink to choose the devices from which the selected classification profile must be deleted.</li> <li>5. Click <b>Submit</b>. You can view the status of the delete operation by clicking the Job Details pop up window.</li> </ol>
Delete user defined action profiles	<ol style="list-style-type: none"> <li>1. Choose <b>Configuration &gt; QoS &gt; Action Profiles</b>.</li> <li>2. Select the action profile you want to remove from the devices as well as from Cisco EPN Manager .</li> <li>3. Click the <b>X</b> (delete) icon in the task bar.</li> <li>4. Alternatively, you can click the device hyperlink to choose the devices from which the selected action profile must be deleted.</li> <li>5. Click <b>Submit</b>. You can view the status of the delete operation by clicking the Job Details pop up window.</li> </ol>

## Launch Cisco Transport Controller to Manage Cisco NCS and Cisco ONS Devices

The Cisco Transport Controller (CTC) is the software interface for a subset of Cisco ONS and Cisco NCS devices. CTC is a Java application that resides on the control cards. It is used to provision and administer these devices.

You can launch CTC from Cisco EPN Manager. Only the latest CTC release is launched, regardless of the NE release you selected. If you need to use other CTC releases, launch CTC from a web browser and connect directly to the NE that has the required CTC release.

To launch CTC:

### Before you begin

Make sure the devices are properly configured to launch CTC. See [Configure Devices So They Can Be Modeled and Monitored, on page 34](#).

- 
- Step 1** From the left sidebar, choose **Inventory > Device Management > Network Devices**.
- Step 2** Click the “i” icon next to the Cisco ONS or Cisco NCS device’s IP address to launch the Device 360 view.
- Step 3** In the Device 360 view, choose **Actions > Launch CTC**. The CTC launcher application is downloaded to your computer. Note that this action will be disabled if launching CTC is not supported on the selected device type.
- Step 4** In the CTC Launcher window, choose one of the following connection mode:

- Use IP—Connection to the device is established using the device's IP address (default option).
- Use TL1 Tunnel—Connection to the device is established using a TL1 session. You can start a TL1 session from CTC or use a TL1 terminal. Note- Use this option to connect to the device that resides behind the third-party OSI-based GNE. The CTC launcher creates a TL1 tunnel to transport the TCP traffic through the OSI-based GNE and the provisioning occurs in CTC

**Step 5** Select the CTC Version, and then click **Launch CTC**.

**Step 6** Enter your CTC credentials.

---



## CHAPTER 13

# Create Templates To Automate Device Configuration Changes

---

See [Configure Devices, on page 267](#) for information on how to configure your devices using out-of-the-box configuration templates that are supplied with Cisco EPN Manager .

- [Why Create New Configuration Templates?, on page 383](#)
- [Ways to Create Configuration Templates Using Cisco EPN Manager , on page 384](#)
- [Create a New CLI Configuration Template Using a Blank Template, on page 384](#)
- [Create a New CLI Configuration Template Using An Existing Template, on page 385](#)
- [Entering Variables in a Template, on page 386](#)
- [Use Global Variables in a Template, on page 390](#)
- [Import and Export a CLI Configuration Template, on page 393](#)
- [Create a New Composite Template, on page 394](#)
- [Create a Shortcut to Your Templates Using Tags, on page 394](#)
- [Deploy Templates to Devices, on page 394](#)
- [Check the Status and Results of a Deployed Configuration Template, on page 399](#)

## Why Create New Configuration Templates?

Cisco EPN Manager provides a number of out-of-the-box configuration templates that you can use to make changes on your network devices. Those are described in [Create a New CLI Configuration Template Using An Existing Template, on page 385](#).

If you have sufficient privileges, you can also create new templates that meet the exact needs of your environment, and then make those templates available for others to use. You can make the templates as simple or as complex as needed, including grouping multiple templates together into a composite template. Finally, you can associate templates with particular devices by creating configuration groups.

Cisco EPN Manager provides out-of-the-box CLI commands that you can use in your templates. It also provides a blank CLI template you can use to create new CLI commands. You can use them singly or with other commands in a composite template.

How you use configuration templates can depend on factors such as how large your network is, the number of designers in your organization, and how much variation there is among devices configuration. For example:

- For a small network with only one or two designers and a limited number of device configurations, start by copying the CLI configurations you know are “good” into a set of templates. You could then combine them into composite templates and make them available to your operators.
- For a large network with many different device configurations, try to identify the configurations you can standardize. This lets you control the amount of exceptions to these standards, and lets you turn features on and off as needed.

## Ways to Create Configuration Templates Using Cisco EPN Manager

Cisco EPN Manager provides different methods for creating new configuration templates, depending on your user account privileges. *CLI configuration templates* contain one or more CLI configuration commands (the same commands you would type when configuring a device). *Composite configuration templates* are comprised of two or more CLI or composite configuration templates. You can specify the order in which the commands are deployed to devices.

- Modify one of the out-of-the-box CLI templates. See [Create a New Composite Template, on page 394](#).
- Use the blank CLI template and enter code by hand. See [Create a New CLI Configuration Template Using a Blank Template, on page 384](#).
- Use the blank CLI template and copy and paste code from a command line configuration session, CLI script, or other stored set of configuration commands. See [Create a New CLI Configuration Template Using An Existing Template, on page 385](#).
- Merge several existing out-of-the-box or user-defined templates into a single template. You specify the order in which the templates contained in the composite template are deployed to devices. See [Create Configuration Groups for Deploying Templates to Groups of Devices, on page 395](#).

Once you have created a set of templates, you can export and import them.

## Create a New CLI Configuration Template Using a Blank Template

Use templates to define a set of reusable device configuration commands. A description of CLI templates and how you can use them is displayed in the web GUI when you choose **Configuration > Templates > Features & Technologies**, then choose **CLI Templates**.

If you want to edit a template that is provided with Cisco EPN Manager, make a copy of the template, give it a new name, and then edit it. See [Create a New CLI Configuration Template Using An Existing Template, on page 385](#).

Templates that you create are stored under **My Templates**.

### Before you begin

Configuration templates are not supported by default on Cisco Optical Networking devices. To enable configuration templates support, select an existing pre-defined CLI configuration template, and in its Device Type section, enable the Optical Networking checkbox. Save this CLI template as a new template. The template is now saved as a user-defined template which lists all optical networking devices such as Cisco NCS 2000, Cisco NCS 4000 devices, and so on.

- 
- Step 1** Choose **Configuration > Templates > Features & Technologies**.
- Step 2** Expand **CLI Templates**, then choose **CLI**.
- Step 3** In the **Template Basic** area:
- Enter a meaningful name for the template. Templates are listed alphabetically in the web GUI.
  - (Optional) Enter a short description that describes how the template should be used—for example, "enable traps on IOS devices."
  - (Optional) Tag the template with an intuitive name. For information on tags, choose **My Tags**.
  - (Cisco IOS only) Enter the device operating systems on which the template can be executed (for example, 12.2 or 15.3). When you execute the template, older device OS versions are filtered out. If you leave this field blank, the template will be applied all OSs for the specified devices.
- Step 4** In the **Validation Criteria** area, specify the devices on which the template can be executed. What you enter here determines which devices are displayed (and can be selected) when you execute the template. You can specify a device family, series, or type.
- Step 5** Specify the device configuration commands in the **Template Detail** area.
- Enter or paste the copied code into the **CLI Content** field. You can copy code from a command line configuration session, CLI script, or other stored set of configuration commands. You must enter code using Apache VTL (see <http://velocity.apache.org/engine/devel/vtl-reference-guide.html>).
  - Configure your variables using the **Managed Variables** dialog. Variables will prompt you for a value when you execute the template.
    - To create a variable using a name in the code, select the code (no spaces) and click the + sign at the top right of the **CLI Content** area. This creates a new (unconfigured) variable by that name in the **Managed Variables** dialog.
    - Click the + sign at the top right of the **CLI Content** area. This adds a blank row to the **Managed Variables** dialog.
- For information about creating variables, see [Entering Variables in a Template, on page 386](#).
- To see how the variable will be displayed when the template is executed, click **Form View**.
  - To save your variables, click **Add to CLI**.
- Step 6** Save your template. Click **Save as New Template**, specify the folder (in **My Templates**) in which you want to save the template, then click **Save**.
- 

## Create a New CLI Configuration Template Using An Existing Template

The easiest way to create a new configuration template is to find a similar existing template, copy it, and edit it. You can also use this procedure to edit templates that you created. (You can only edit templates that you create.)

- 
- Step 1** Choose **Configuration > Templates > Features & Technologies**.
- Step 2** Expand **CLI Templates**, then choose **System Templates - CLI**.

- Step 3** In the Template navigation panel on the left, locate the template you want to copy, hover your mouse cursor over the icon that is displayed next to the template name, then click **Duplicate** in the popup window.
- Step 4** In the **Duplicate Template Creation** dialog, specify a name and the folder (under **My Templates**) where you want the new template to be saved, and click **OK**.
- For example, if you copy a template that resides under **CLI Templates > System Templates - CLI**, by default the template is saved under **My Templates > CLI Templates > System Templates - CLI (User Defined)**.
- Step 5** Add the validation criteria and CLI content as described in [Create a New CLI Configuration Template Using a Blank Template, on page 384](#).

## Entering Variables in a Template

These topics provide information that will help you when entering variables into a template:

- [Data Types, on page 386](#)
- [Manage Database Variables in CLI Templates, on page 387](#)
- [Use Validation Expressions, on page 387](#)
- [Add Multi-line Commands, on page 388](#)
- [Add Enable Mode Commands, on page 389](#)
- [Add Interactive Commands, on page 389](#)

## Data Types

[Table 1](#) lists data types that you can configure in the Manage Variables page.

Data Type	Description
String	Enables you to create a text box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
Integer	Enables you to create a text box that accepts only numeric value. If you want to specify a range for the integer, expand the row and configure the Range From and To fields. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
DB	Enables you to specify a database type. See the <a href="#">Manage Database Variables in CLI Templates, on page 387</a> .
IPv4 Address	Enables you to create a text box that accepts only IPv4 addresses for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
Drop-down	Enables you to create a list for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field (with a comma-separated value for multiple lists which appears in the UI).



Check box	Enables you to create a check box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field.
Radio Button	Enables you to create a radio button for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field.
Text Area	Enables you to create a text area which allows multiline values for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.

## Manage Database Variables in CLI Templates

You can use database (DB) variables for the following reasons:

- DB variables are one of the data types in CLI templates. You can use the DB variables to generate device-specific commands.
- DB variables are predefined variables. To view the list of predefined DB variables, see the `CLITemplateDbVariablesQuery.properties` file at the following location:  
folder/opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate.
- For example, SysObjectID, IPAddress, ProductSeries, ImageVersion are DB variables. When a device is added to Cisco EPN Manager, the complete details of the device is collected in the DB variables. That is, the OID of the devices is collected in SysObjectID, product series in ProductSeries, image versions of the device in ImageVersion, and so on.
- Using the data collected by the DB variables, accurate commands can be generated to the device.
- You can select the DB variable in the Type field (using the Managed Variables page). Expand the name field and fill in the default value field with any of the DB variables which you want to use.
- When a device is discovered and added to Cisco EPN Manager, you can use the database values that were gathered during the inventory collection to create CLI templates.



**Note** While it is possible to create a customized query using Enterprise JavaBeans Query Language (EJB QL), only advanced developers should attempt this. We recommend you use the variables defined in the `CLITemplateDbVariablesQuery.properties` file only.

## Use Validation Expressions

The values that you define in the Validation Expression are validated with the associated component value. For example, if you enter a default value and a validation expression value in the design flow, this will be validated during the design flow. That is, if the default value does not match with the entered value in the validation expression, you will encounter a get error at the design flow.



**Note** The validation expression value works only for the string data type field.

For example, choose **Configuration > Templates > Features and Technologies**, then choose **CLI Templates > CLI**. In the Template Detail area, click the **Add Variable** tab to view the list of Variables. Click the Add plus sign (+) in the Add Variables tab to add a row to the CLI template. Choose String in the Type field, enter the remaining values, and click **Save**. From the list of variables, expand the details of this new variable and configure the regular expression, which will not allow a space in that text box. Enter the following expression in the Validation Expression field.

```
^[\S]+$
```

Default value (optional)—ncs

The value should match with regular expression in the validation expression field.

Save the template, and then select a device. Try to enter a space in the text field. You will encounter a regular expression error.

## Add Multi-line Commands

To enter multi-line commands in the CLI Content area, use the following syntax:

```
<MLTCMD>First Line of Multiline Command
Second Line of Multiline Command
.....
.....
Last Line of Multiline Command</MLTCMD>
```

where:

- <MLTCMD> and </MLTCMD> tags are case-sensitive and must be entered as uppercase.
- The multi-line commands must be inserted between the <MLTCMD> and </MLTCMD> tags.
- The tag cannot be started with a space.
- The <MLTCMD> and </MLTCMD> tags cannot be used in a single line.

Example 1:

```
<MLTCMD>banner motd Welcome to
Cisco. You are using
Multi-line commands.
</MLTCMD>
```

Example 2:

```
<MLTCMD>banner motd ~ ${message}
</MLTCMD>
```

where {message} is a multi-line input variable.

### Restrictions for Using Multi-Line Banner Commands

Cisco EPN Manager does not support multi-line banner commands. You can use *banner file xyz format* as shown in the following example.

```
#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
(config)#parameter-map type webauth global
(config-params-parameter-map)# type webauth
(config-params-parameter-map)#banner file tftp://209.165.202.10/banner.txt
(config-params-parameter-map)#^Z
#more tftp://192.168.0.0/banner.txt
Disclaimer:
Usage of this wireless network is restricted to authorized users only.
Unauthorized access is strictly forbidden.
All accesses are logged and can be monitored.
#
```

## Add Enable Mode Commands

Use this syntax to add enable mode commands to your CLI templates:

```
#MODE_ENABLE<<commands >>#MODE_END_ENABLE
```

## Add Interactive Commands

An interactive command contains the input that must be entered following the execution of a command.

To enter an interactive command in the CLI Content area, use the following syntax:

```
CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question
2<R>command response 2
```

where <IQ> and <R> tag are case-sensitive and must be entered as uppercase.

For example:

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

### Combining Interactive Enable Mode Commands

Use this syntax to combine interactive Enable Mode commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

For example:

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>XXX
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

### Adding Interactive Multi-line Commands

This is an example of an interactive command that contains multiple lines:

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
@</MLTCMD>
#ENDS_INTERACTIVE
```

## Use Global Variables in a Template

Cisco EPN Manager enables you to deploy customized CLI configuration to your devices by creating CLI templates which contain these customized configuration options. When you create CLI templates or modify existing ones, you can define the content of the template using global and/or template variables.

- Template variables: allow you to input values to the variable during CLI template or service creation.
- Global variables: are predefined and associated with the CLI template or with a service at a global level (by default). You cannot view a global variable or input its values during service creation.

All variables names start with words that identify them as global or template variable. Global variables are accessible to all Cisco EPN Manager templates such as CLI templates or Composite templates. They identify the type of service (CE, L3VPN, CEM, etc.) that the variable can be associated with. If you create a new global variable, you must ensure that you specify a name that starts with the letters 'gv' followed by other words that promote easy identification of the variable. Global variables that you create, can be further edited and deleted. The global variables available in Cisco EPN Manager by default, cannot be edited or deleted.

While global variables are applicable to all template types, the variables created specifically during CLI template creation are applicable to that template alone. These variables created during CLI template creation cannot be associated with other CLI templates.

In the CLI template configuration example shown below, 'gv.service-ethernet-mainInterfaceName' represents the global variable. If this template is associated with a service, then during service creation, the dynamic part of the global variable, 'mainInterfaceName', is replaced by the values (such as the ethernet interface, in case of CE services) specified in the service. However, you will not be able to view or modify this global variable during service creation. '\$descr' is a static value which represents the template variable. During service creation, this template variable will enable you to modify or specify a value of the type String (for the description field).

```
interface $gv.service-ethernet-mainInterfaceName
    description $descr
exit
```

To use global variables to create CLI templates:

- 
- Step 1** Choose **Configuration > Templates > Global Variable** to create new global variables.
- To use existing global variables that are pre-populated in Cisco EPN Manager for each service type (CE, L3VPN, and CEM), skip to Step 4.
- Step 2** Click the Add '+' icon. To edit existing variables, select the global variable and click the Edit button.
- Step 3** Specify the following parameters and click **Save**. Your changes are saved in the Cisco EPN Manager database and are not immediately deployed to the device.
- **Name:** Enter a unique name for the variable ensuring that the name starts with the letters 'gv' followed by the type of service this global variable is relevant to. You can use special characters such as the dot, hyphen, and underscore.
  - **Description:** Enter a unique description for easy identification of the variable. This description is extremely important to help identify the purpose of this variable that may be used in CLI templates. The CLI templates could further be used to provision services (such as L2 and L3 services). And on the service creation page, you will rely completely on the variable description to identify the purpose of the variable.
  - **Type:** Use one of the following options to specify the type of variable:
    - **String:** Enables you to create a text box for CLI templates. Only the string type of variable is applicable to CLI templates used in service provisioning.
    - **Integer:** Enables you to create a text box that accepts only numeric value. It can later be configured to specify a range for the value.
    - **IPv4 Address:** Enables you to create a text box that accepts only IPv4 addresses for CLI templates.
    - **Drop-down:** Enables you to create a drop-down list for CLI templates.
    - **Check box:** Enables you to create a check box field for CLI templates.
    - **Radio Button:** Enables you to create a radio button for CLI templates.
    - **Text Area:** Enables you to create a text area which allows multiline values for CLI templates.
  - **Value:** Specify the values that must be generated based on the selected Type values explained above. If you want to specify the value during service creation or during CLI template creation, you can choose 'Not Available' as a place holder.
  - **Display Label:** Enter how you want the variable to be displayed in the Cisco EPN Manager GUI.

**Step 4** Associate the global variable with a CLI template:

- Navigate to **Configuration > Templates > Features & Technologies**.
- To create a new CLI template from scratch, see [Create a New CLI Configuration Template Using a Blank Template, on page 384](#).
- To associate global variables with existing templates, see [Create a New CLI Configuration Template Using An Existing Template, on page 385](#).
- To add global variables, from the Template Details section, use the **Add Global Variable** search field to locate the global variable. For easy identification, you can also use the **Global Variable** hyperlink displayed at the top right corner of the page. You can use global variables along with CLI, and/or template variables in the same CLI template.

You can identify the services that the variables belong to by looking at the variable name. Variables applicable to CE services, have variable names that start with the letters 'gv.ce-service-ethernet\*'. Variables applicable to L3VPN services, have variable names that start with the letters 'gv.l3vpn-service-l3vpn\*'. These variables can be associated with new or existing CLI templates.

- Make the required changes to the CLI template and click **Save as New Template**.
- The CLI template is now saved and displayed under **My Templates > CLI Templates (User Defined)**.
- (Optional) Deploy the CLI template to the devices as explained in [Deploy Templates to Devices, on page 394](#).

**Step 5** (Optional) To provision services (L2, L3VPN, CEM, Flex LSP, Layer 3 link) using CLI templates (associated with global and template variables), see, [Extend a Circuit/VC Using Templates, on page 512](#).

### Example

Sample Global Variables Available in Cisco EPN Manager :

- Following are the sample global variables that can be used with L3VPN services:

<input type="checkbox"/>	gv.service-l3vpn-bgpASNumber	BGP AS Number	String
<input type="checkbox"/>	gv.service-l3vpn-bgpNeighborASNumberList	BGP Neighbor AS Number	String
<input type="checkbox"/>	gv.service-l3vpn-bgpNeighborAddressFamili...	Neighbor Address Family	String
<input type="checkbox"/>	gv.service-l3vpn-bgpNeighborsList	BGP Neighbor	String
<input type="checkbox"/>	gv.service-l3vpn-bgpRouterId	BGP Router ID	String
<input type="checkbox"/>	gv.service-l3vpn-bridgeDomainIdList	Bridge Domain ID	String
<input type="checkbox"/>	gv.service-l3vpn-egressServiceQoSPolicyN...	Egress Service QoS Policy Name	String
<input type="checkbox"/>	gv.service-l3vpn-egressUNIQoSPolicyName	Egress UNI QoS Policy Name	String
<input type="checkbox"/>	gv.service-l3vpn-ingressServiceQoSPolicyN...	Ingress Service QoS Policy Name	String
<input type="checkbox"/>	gv.service-l3vpn-ingressUNIQoSPolicyName	Ingress UNI QoS Policy Name	String
<input type="checkbox"/>	gv.service-l3vpn-mainInterfaceNameList	Main Interface Name	String
<input type="checkbox"/>	gv.service-l3vpn-serviceInterfaceNameList	Sub-Interface or BDI/BVI Name	String
<input type="checkbox"/>	gv.service-l3vpn-vrfAddressFamilyList	VRF Routing Address Family	String
<input type="checkbox"/>	gv.service-l3vpn-vrfName	VRF Name	String

- Following are the sample global variables that can be used with CEM services:

gv.service-cem-auNumber	AU (AU-3 or AU-4) number	String
gv.service-cem-cemFrameType	CEM frame type	String
gv.service-cem-cemGroupNumber	CEM group number	String
gv.service-cem-cemGroupNumberList	CEM group number list for local connects	String
gv.service-cem-cemInterfaceName	CEM interface name	String
gv.service-cem-cemInterfaceNameList	CEM interface name list for local connects	String
gv.service-cem-controllerInterfaceName	Controller name	String
gv.service-cem-e1Number	E1 number	String
gv.service-cem-l2vpnContextName	L2VPN context name	String

## Import and Export a CLI Configuration Template

These topics explain how to export and import configuration templates. Templates can be exported templates have an .xml file name; multiple templates are exported as a zip file.

- If you export multiple configuration templates, the .xml files are placed in a zip file with the prefix name **Exported Templates**.
- Single files are exported and imported as .xml files
- You can import multiple .xml files by selecting individual files or by importing a zip file.
- When you import CLI templates, the user-defined global variables that are part of the file are not imported automatically. You need to add these variables to the CLI template manually.

---

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

**Step 2**

**Step 3** To export a configuration template:

- a)
- b) Select the template(s) that you want to export and click **Export**.
- c) Save the files as the desired location.

**Step 4** To import a configuration template:

- a) Under the **CLI Templates** folder, hover your mouse cursor over the "i" next to **CLI**.
  - b) Click **Show All Templates**, then click **Import**.
  - c) In the **Import Templates** dialog box, choose the **My Templates** folder where you want to import the templates, then click **Select Templates** and navigate to the file you want to import.
  - d) Confirm your choices, then click **OK**.
-

## Create a New Composite Template

All out-of-the-box and user-created templates can be added to a single composite template, which aggregates all of the individual feature templates that you need. When you create a composite template, you can also specify the order in which member templates should be executed. You can use composite templates to make changes to single or groups of devices.

- 
- Step 1** Choose **Configuration > Templates > Features & Technologies**.
- Step 2** Expand the **Composite Templates** folder and choose **Composite Templates**.
- Step 3** In the **Template Basic** area, enter a name for the template.
- Step 4** In the **Validation Criteria** area, choose the devices to which all of the templates contained in the composite template should apply. For example, if your composite template contains one template that applies to Cisco ASR 900 series routers and another that applies to all routers, you only need to choose **Routers > Cisco ASR 900 Series Aggregation Services Routers** from the Device Type list. If a device type is dimmed, the template cannot be applied on that device type.
- Step 5** In the **Template Detail** area, choose the templates to include in the composite template. Using the arrows, place the templates in the in the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the interface template.
- Step 6** Click **Save as New Template**. After you save the template, and apply it to your devices (see ).
- 

## Create a Shortcut to Your Templates Using Tags

When you apply a tag to a template, the template is listed under the **My Tags** folder. Tagging a configuration template helps you:

- Search a template using the tag name in the search field
- Use the tagged template as a reference to configure more devices

To tag an existing template, follow these steps:

- 
- Step 1** Choose **Configuration > Templates > Features & Technologies**.
- Step 2** Expand the **My Templates** folder and choose the template that you want to tag.
- Step 3** Enter a tag name in the **Tag as** text box, then click **Save**.
- 

## Deploy Templates to Devices

These topics describe the ways you can deploy (run) groups of commands on devices using configuration templates:

- [Create Configuration Groups for Deploying Templates to Groups of Devices](#)
- [Deployment Flow for Configuration Templates Using the Wizard](#)
- [Deployment Flow for CLI Templates using the Wizard](#)



- [Deployment Flow for Composite Templates Using the Wizard](#)
- [Deploy Templates to Devices Without Using Configuration Groups](#)

## Create Configuration Groups for Deploying Templates to Groups of Devices

If you have devices that require the same configuration, you can create a *configuration group* that contains devices and templates that can be applied to those devices. Creating a configuration group allows you to quickly apply new templates without remembering to which devices the new templates should be deployed.

Composite templates allow you to group smaller templates together, but configuration groups specify the *relationship* between the templates and the groups of devices, and the order in which commands are executed.

- 
- Step 1** Choose **Configuration > Templates > Configuration Groups**.
- Step 2** In the Configuration Group Basic area, enter a name.
- Step 3** To display devices from which you can make selections, in the Template Selection area, add one or more templates by clicking **Add** and selecting the templates. This also populates the Device Type field.
- Step 4** Add additional templates by clicking **Add** in the Template Selection area. You cannot choose templates that are mutually-exclusive; for example, you cannot choose Add-Host-Name-IOS and Add-Host-Name-IOS-XR.
- Step 5** Select the devices on which you want to deploy the template, then click **Next** to choose the input option.
- Step 6** In the Device Selection area, select the devices you want to add to the configuration group.
- Step 7** If you have multiple templates, the order in which templates will be listed by selecting one and clicking the up or down arrow.
- Step 8** Click **Save as New Configuration Group**.
- 

## Deployment Flow for Configuration Templates Using the Wizard



---

**Note** This deployment flow is not applicable for Controller based templates.

---

- 
- Step 1** After you create a configuration template, click **Deploy**. The Deployment wizard page opens.
- Step 2** Select the devices on which you want to deploy the template, then click **Next** to choose the input values.
- Step 3** In the **Input Values** tab, you can toggle between the **Form** and **CLI** view.
- Step 4** After entering the necessary configuration values, click **Next** or click **CLI** to confirm the device and template configuration values.
- Step 5** Schedule the deployment job using **Schedule Deployment** tab, if required:
- Create a meaningful deployment job name, then specify whether to run the now or in the future.
  - You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
  - You can configure the following job options:  
Failure Policy:

- **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
- **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
- **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
- **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

- Step 6** Click **Next** to view the job deployment summary.
- Step 7** On the **Deployment Summary** tab, you will see the CLI view for each of the device.
- Step 8** Click **Finish** to deploy the template.
- Step 9** Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

## Deployment Flow for CLI Templates using the Wizard

- Step 1** After creating the CLI template, click **Deploy**. The Deployment wizard page opens.
- Step 2** Select the devices on which you want to deploy the template, then click **Next** to choose the input option.
- Step 3** Select the devices on which you want to deploy the template from the **Add devices** table. The selected devices appear in the **Devices to deploy** table.
- Step 4** Select the mode in which you want to deploy the template. The options are **Work Flow** and **Export/Import CSV**.
- Step 5** Click the **Work Flow** option and click **Next**. See *Step 6*.
- Step 6** Alternately, click **Export/Import CSV** option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.
- Uncheck the **Do you want Optional Parameters** check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
  - Click **Export CSV** to download the CSV template to your local system.
  - Enter the configuration values for each specific device in the downloaded CSV template.
  - Click **Import CSV** to upload the updated CSV file. The input values automatically gets updated.
  - Click **Next** to input values.
- Step 7** In the **Input Values** tab, you can toggle between **Form** and **CLI** view. Configure the following in the Input Values tab:
- Enter all the mandatory fields for each template, then click **Apply**.  
If the validation is successful, then the border of the circle around the selected template changes to green.
- Step 8** After entering the necessary configuration values, click **Next** or **CLI** to confirm the device and template configuration values.
- Step 9** Schedule the deployment job using **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

Failure Policy:

- **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
- **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
- **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
- **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

- Step 10** Click **Next** to view the job deployment summary.
- Step 11** On the **Deployment Summary** tab, you will see the CLI view for each of the device.
- Step 12** Click **Finish** to deploy the template.
- Step 13** Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

## Deployment Flow for Composite Templates Using the Wizard

- Step 1** Choose **Configuration > Templates > Features & Technologies > Composite Templates > Composite Templates**.
- Step 2** Enter the required information in the Template Basic section.
- Step 3** In the Template Detail section, choose the templates to include in the composite template, and click **Save as New Template**.
- Step 4** After creating the composite template, click **Deploy**. The Deployment wizard page opens.
- Step 5** Select the devices on which you want to deploy the template.
- Step 6** Select the devices on which you want to deploy the template from the **Add devices** table. The selected devices appear in the **Devices to deploy** table.
- Step 7** Select the mode in which you want to deploy the template. The options are **Work Flow** and **Export/Import CSV**.
- Step 8** Click the **Work Flow** option and click **Next**. See *Step 6*.
- Step 9** Alternately, click **Export/Import CSV** option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.
- Uncheck the **Do you want Optional Parameters** check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
  - Click **Export CSV** to download the CSV template to your local system.
  - Enter the configuration values for each specific device in the downloaded CSV template.

- d) Click **Import CSV** to upload the updated CSV file. The input values automatically get updated.
- e) Click **Next** to input values.

**Step 10** In the **Input Values** tab, you can toggle between **Form** and **CLI** view. Configure the following in the Input Values tab:

- a) Select templates for a device from the navigation widget. To select templates, click the circle (T1, T2, T3, T4, T5 ...) in the upper right corner. If there are more than five templates, click three dots. The drop-down list will pop-up with all the available templates.
- b) Enter all the mandatory fields for each template, then click **Apply**.

If the validation is successful, then the border of the circle around the selected template changes to green and green tick mark appears adjacent to the selected templates for the available templates in the popup.

**Step 11** After entering the necessary configuration values, click **Next** or **CLI** to confirm the device and template configuration values.

**Step 12** Schedule the deployment job using **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

Failure Policy:

- **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
- **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
- **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
- **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

**Step 13** Click **Next** to view the job deployment summary.

**Step 14** On the **Deployment Summary** tab, you will see the CLI view for each of the device.

**Step 15** Click **Finish** to deploy the template.

**Step 16** Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

## Deploy Templates to Devices Without Using Configuration Groups

Once a template is saved, it can be deployed (run on) devices. You can deploy a template from the **Configuration > Templates > Features & Technologies** navigation area, or by using Configuration Groups, which is launched from **Configuration > Templates > Configuration Groups** (see [Create Configuration Groups for Deploying Templates to Groups of Devices](#), on page 395).

To deploy a customized or system template from the **Features & Technologies** navigation area:

- 
- Step 1** Choose **Configuration > Templates > Features & Technologies**
- Step 2** Expand the drawer that contains the template(s) you want to deploy.
- Step 3** Choose the templates you want to deploy, and click **Deploy**.
- Step 4** In the **Template Deployment** window, check the settings and schedule and click **OK**.
- 

## Check the Status and Results of a Deployed Configuration Template

When you deploy a configuration template, Cisco EPN Manager displays a dialog box with a hyperlink that directs you to the Jobs window. From here you can:

- View the results of the command by clicking the History tab and expanding the job instance.
- Repeat the deployment, or schedule it for a later time
- Manage the job (delete it, pause it, resume it, and so forth).





## CHAPTER 14

# Manage Cable Devices

- [Manage Cable Devices, on page 401](#)
- [Cable Management Features and Supported User Groups, on page 402](#)
- [Configure Client Credentials for Cable Devices, on page 405](#)
- [Add Cable Devices, on page 406](#)
- [Manage Cisco cBR-8 and RPDs Association, on page 406](#)
- [View and Export Cable Device Information and Configuration Details, on page 408](#)
- [Monitor the Health of RPD to cBR-8 Links, on page 410](#)
- [View the Cable Dashboard, on page 411](#)
- [Visualize the Topology of Cable Devices on the Network Topology, on page 411](#)

## Manage Cable Devices

The Cisco cBR-8 Converged Broadband Router (Cisco cBR-8) is a 13 rack unit (RU) chassis. It supports multiple card modules and is designed with back-to-back midplanes; a front facing Digital Midplane and a rear facing RF Midplane. In a cable network with the Remote PHY architecture, multiple Remote PHY Devices (RPDs) connect to Cisco cBR-8 devices based on the Data Over Cable Systems Interface Standard (DOCSIS) and EuroDOCSIS standards that define two-way operation over the cable network.

Remote PHY is an architectural strategy that removes the PHY element from a product and places that PHY element in a separate access point interconnected with an IP network. The Cisco Remote-PHY solution leverages existing IP technologies like Ethernet PON (EPON), Gigabit-capable Passive Optical Networks (GPON), and Metro Ethernet (MetroE) equipment; it deploys DOCSIS in Multi Dwelling Units (MDUs) over digital fiber to enable two-way services over cable.

Using Cisco EPN Manager, you can add and discover Cisco cBR-8 and devices and RPDs, view their L2TP links and topology on the network topology, and further configure them. You can also continuously monitor the health of RPDs to Cisco cBR-8 device links. See [Manage Cisco cBR-8 and RPDs Association, on page 406](#).

For more information about cBR-8 devices, see <http://www.cisco.com/c/en/us/td/docs/cable/cbr/cisco-cbr/index.html>:

The process of managing cable devices in Cisco EPN Manager involves:

1. Ensuring that the cBR-8 devices, and Cisco Smart PHY are up and available for configuring.
2. Adding the cBR-8 device and ensuring that the inventory collection status for the device is 'Completed'. See [Add Devices to Cisco EPN Manager, on page 44](#)

3. (Optional) Configuring the required access in Cisco EPN Manager by providing Cisco Smart PHY credentials.
4. (Optional) Monitoring the devices using the network topology to view the associated monitoring policies, alarms information, and link information.
5. (Optional) Managing device images using Software Image Management. See [Manage Device Software Images, on page 107](#).

## Features and Limitations

Cisco EPN Manager supports the following features to manage cable devices:

- Configuring Cisco Smart PHY with Cisco EPN Manager .
- Monitoring and visualizing RPD to cBR-8 L2TP links in the network topology.
- Ability to place unmapped cable devices on the network topology.
- Managing software images on cBR-8 devices.
- Performing configuration audit using compliance for cBR-8 devices.
- Viewing cBR-8 device 360 and interface 360 information.
- Viewing cBR-8 device details in the chassis view.
- Viewing cable device syslogs.

Cisco EPN Manager has the following limitation in managing cable devices:

- You cannot set the location of devices in bulk using the **Import and Export Locations** options on the network topology.
- Cisco Smart PHY must not be configured with more than one Cisco EPN Manager server. You must also ensure that after you configure the Cisco Smart PHY client credentials in the Admin Settings page, you must not change the configuration to a new client.

## Cable Management Features and Supported User Groups

The following table lists the various cBR-8 and RPD management tasks supported by Cisco EPN Manager and the supported user groups. See [View and Change the Tasks a Group Can Perform, on page 676](#) for information on the tasks that pertain to each user group and the default settings.



Table 26: Cable Management Features and Supported User Groups

Cable Management Features	Root/Super Users	Admin Users	Config Managers	System Monitoring	Monitor Lite	User Assistant	NBI Credentials	North-bound NBI	NBI Read	NBI Write	Other Users
Adding, editing, deleting, and importing RPDs. Editing RPD data using the inline editing option.	Yes	Yes	Yes	—	—	—	—	—	—	Yes (not applicable for inline editing of RPD data.)	—
Viewing the Cable RPD Association page.	Yes	Yes	Yes	Yes	Yes	Yes	—	—	—	—	—
Listing RPDs.	Yes	Yes	Yes	Yes	Yes	—	—	—	Yes	—	—
Exporting RPDs.	Yes	Yes	Yes	Yes	Yes	—	—	—	—	Yes	—
Using quick launch hyperlinks. From the Cable RPD Association page to the network topology and vice versa.	Yes	Yes	Yes	—	—	—	—	—	—	—	—
Viewing cable devices in the network topology	Yes	Yes	Yes	Yes	Yes	—	—	—	—	—	—

Cable Management Features	Root/Super Users	Admin Users	Config Managers	System Monitoring	Monitor Lite	User Assistant	NBI Credentials	North-bound NBI	NBI Read	NBI Write	Other Users
Launching, viewing, adding, and editing Cable Application (Cisco Smart PHY) client credentials.	Yes	Yes	—	—	—	—	—	—	— (Only viewing details is permitted)	—	—
Viewing Cisco cBR-8 device information (in the Configuration tab) such as the device's license usage status, available sensor readings, IPv4 and IPv6 statistics, voice calls count, fan and power supply status, and other generic data. Also view slot level information such as FPGA/CPLD version numbers.	Yes	Yes	Yes	—	—	—	—	—	Yes	—	—

Cable Management Features	Root/Super Users	Admin Users	Config Managers	System Monitoring	Monitor Lite	User Assistant	NBI Credentials	North-bound NBI	NBI Read	NBI Write	Other Users
View Cisco cBR-8 device performance information (in the Performance tab) in the linecard upstream and downstream dashlet, power supply dashlet, CPU and memory utilization dashlet, fan tray dashlet, along with other general configuration details.	Yes	—	Yes	Yes	—	—	—	—	Yes	—	—

## Configure Client Credentials for Cable Devices

To manage Cisco cBR-8 devices and Cisco Remote-PHY devices (RPDs), you must first configure the Cisco Smart PHY client credentials. This enables Cisco EPN Manager to set up a connection with the Cisco Smart PHY application.

To configure Cisco Smart PHY credentials:

### Before you begin

Ensure that you log in with the required credentials for configuring the Cisco Smart PHY client credentials. For information on the user groups and supported tasks, see [Cable Management Features and Supported User Groups](#), on page 402.

For more information about Cisco Smart Phy, see [https://www.cisco.com/c/en/us/td/docs/cable/cbr/administration/guide/cisco\\_smart\\_phy\\_application\\_user\\_guide/information\\_about\\_cisco\\_sdn\\_application.html](https://www.cisco.com/c/en/us/td/docs/cable/cbr/administration/guide/cisco_smart_phy_application_user_guide/information_about_cisco_sdn_application.html).



**Note** The Cisco Smart PHY application must not be configured with more than one Cisco EPN Manager server. You must also ensure that after you configure Cisco Smart PHY client credentials in the Admin Settings page, you must not change the configuration to a new Cable Application client.

- Step 1** From the left sidebar, choose **Administration > Settings > System Settings**.
- Step 2** Expand Client and User and choose **Cisco Smart PHY Credentials**.
- Step 3** Specify the following Cable Application credentials:
- a) IP Address or DNS name—The IPv4 address of the client or the DNS hostname of the Cisco Smart PHY application.
  - b) Port—Numeric port number for communication between the device and Cisco EPN Manager .
  - c) User name and password—Specify the login credentials to login to the client. You will need to re-enter the password for verification.
- Step 4** Click **Save** to enable the client credentials.

## Add Cable Devices

Add the required cBR-8 devices to Cisco EPN Manager by device discovery, manual addition, or by importing device details using a CSV file. For more information about adding devices, see [Add Devices to Cisco EPN Manager](#) , on page 44.

After you add devices, and before you configure cable devices, you must first ensure that the inventory collection status for the devices is **Completed**. You can then proceed with adding RPDs and associating them with the cable devices. See [Manage Cisco cBR-8 and RPDs Association](#), on page 406.

## Manage Cisco cBR-8 and RPDs Association

You can use Cisco EPN Manager to monitor and discover RPDs from Cisco cBR-8 devices. Once the devices are discovered, the pairing between the devices must be established as explained in the sections below.

Launch the Cable RPD Association page in one of the following ways:

- From the **Configuration > Network Devices > Cable RPD Association** option in the left navigation panel.
- From the **Cable** drop-down menu in the network topology.

**RPD Auto Discovery:** As part of the Cisco cBR-8 device discovery, RPDs associated with the devices are automatically added to the Cisco EPN Manager database. In this scenario, you do not need to add or import the RPDs as shown below.

Before you can manage Cisco cBR-8 devices and RPDs, you need to first discover the cBR-8 - RPDs pairing information to Cisco EPN Manager from the Cisco cBR-8 devices.

When Cisco cBR-8 devices are in sync with Cisco EPN Manager with a pending integration with the Cisco Smart PHY, the auto discovered service templates (associated with RPDs) cannot be edited. Once the integration

with the Cisco Smart PHY is complete, the service templates that are marked None are auto assigned to the default service template.



**Note** If RPDs auto-discovered from Cisco cBR-8 devices do not have pre-configured RPD names, then Cisco EPN Manager displays these RPD names in the format RPD-**<Mac address>**. However, if Cisco EPN Manager is integrated with the Cisco Smart PHY, then it displays the RPD names as configured in the Cisco Smart PHY application.

**Link Utilization:** After the pairing of the devices has been established, you can view the topology of the cable network in the network topology and monitor the health of the links between the devices. To do this:

1. Choose **Maps > Topology Maps > Network Topology**.
2. Use the **Cable** drop-down menu to filter Cable devices. By default, the physical links between the Cisco cBR-devices and the RPDs are displayed.
3. Use the **Show** option and choose **Links** to filter Physical or L2TP links.

For cable L2TP links, L2TP utilization (for available L2TP tunnels) is calculated per RPD by getting the OFDM channels utilization of the associated downstream controller. For more information, see, [Show Bandwidth Utilization for Links on the Map, on page 166](#).

**Pre-requisites:**

- Add cBR-8 devices to Cisco EPN Manager . See [Add Devices to Cisco EPN Manager , on page 44](#).
- Ensure that the inventory collection status for the cBR-8 device (associated with the RPDs you are importing) is 'Completed'.
- Ensure that you configure the Cisco Smart PHY client credentials. See [Configure Client Credentials for Cable Devices, on page 405](#).

## RPD Device Parameters and Descriptions

RPD Device Parameters	Description
RPD Name	Hostname of the RPD device.
RPD MAC ID	MAC ID of the RPD.
Associated cBR-8	Cisco cBR-8 device that the selected RPD is linked to.
Interface	Interface of the cBR-8 device that is physically connected to the RPD.
Service Templates	Cisco EPN Manager cable service template applied to the RPD. When field is left blank during the import operation, the default service template is assigned to the RPD automatically. When the Cisco Smart PHY client is not configured, this field is marked 'Unknown'.
Latitude and Longitude	Represents the exact location of the RPD. This then helps visualize the location of the device on the Cisco EPN Manager Network Topology.

RPD Device Parameters	Description
Information (i) icon	The information (i) icon allows you to launch the device 360 view for the selected Cisco cBR-8 device and its associated interfaces. For more information, see, <a href="#">Get Basic Device Information: Device 360 View, on page 63</a> .
Data Service Group	All RPDs with the same data service group will share the Downstream controller for Data Service (Virtual Splitting for Data)
Video Interface	Complete name of the TenGigabitEthernet DPIC Interface to be used for Video (Narrowcast) Service
Additional Cores	List of additional cores the RPD should connect to

## View and Export Cable Device Information and Configuration Details

Using the Cisco EPN Manager Chassis View, you can view Cisco cBR-8 device information such as the device's license usage status, sensor readings, IPv4 and IPv6 statistics, bandwidth utilization on the different channels and controllers, fan and power supply status, and more. You can also view slot level information such as FPGA/CPLD version numbers.

To view device and chassis information described in the table below:

### Before you begin

To ensure that information is collected and reported for the Cisco cBR-8 routers in your network, verify that Cable Policies is listed on the **Monitoring Policies** page (**Monitor > Monitoring Tools > Monitoring Policies > Policies** pane), is currently active, and has polling intervals set for its parameters. To activate Cable monitoring policies, see, [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205](#).

- 
- Step 1** From the left sidebar, choose **Configuration > Network Devices**.
  - Step 2** To view device or chassis information, click the device/chassis/supervisor (SUP) from the Chassis Explorer.
  - Step 3** To view the fan or power supply information, click fan or power supply module from the Chassis Explorer.
  - Step 4** Click the **Configuration** tab.
  - Step 5** Expand the tabs listed in the table below to view the corresponding information.

For a graphical representation of this info, navigate to the **Performance** tab and ensure that you add the required dashlet to the tab. You can display up to 10 dashlets at a given point of time on the Performance tab.

To filter mac domains, fiber nodes, or controllers based on the utilized bandwidth values or the stream types, use the **Advanced Filter** option in the **Configuration** tab. For example, you can filter mac domains that have average utilization values greater or lesser than a particular range. You can further add additional filters to list mac domains with a particular stream type (such as downstream or upstream).

Table 27: Cable Device Configuration Information

Tabs	Chassis Explorer Selection	Requires Policy Activation	Information Available
General	Device, chassis, SUP, fan, and power supply unit.	No	<ul style="list-style-type: none"> <li>Generic device and chassis information: View information such as, device name, IP address, installed software version, system up time, device serial number, product ID, part number, device operational state (whether enabled or not), hardware version number, associated CLEI code, operating or configured redundancy state, the unique description associated with the device, number of ports that are up/down, and the device's current ICMP latency.</li> <li>Fan information: Fan usage status in percentage format.</li> <li>Power Supply information: Total power capacity and power consumed by the device in watts.</li> <li>Line card information: View generic device information and the upstream and downstream bandwidth utilization of the card.</li> </ul>
License Usage Status	Device	No	Licenses usage information and reporting of the Cisco products on the Cisco cBR-8 device, along with the enforced state.
Sensor Readings	Line cards, fans, and power supply units.	Yes	General environmental status of each FRU since installation. You can view the name, sensor state, and threshold values. The sensor readings include the temperature conditions.
FPGA/CPLD Versions	SUPs	No	All available Supervisor FPGA or CPLD firmware on the router and their respective version numbers.
IPv4 and IPv6 Statistics	Device	Yes	Type of packets and number of packets being sent and received. This includes IPv4 ARP statistics, and IPv6 neighbor statistics.
Voice Calls	Device	Yes	This tab displays the count of active high priority calls and all active calls. The count is refreshed periodically based on your settings in the Cable Monitoring policy settings.
Modem Details	Device	Yes	View the number of cable modems using different DOCSIS versions (such as DOCSIS 1.1 and DOCSIS 2.0) and belonging to different vendors.





Tabs	Chassis Explorer Selection	Requires Policy Activation	Information Available
DEPI Sessions	Device	No	<p>DEPI (Downstream External-PHY Interface) is an IP Tunnel that exists between the CCAP Core and the Remote PHY using Layer 2 Tunneling Protocol (L2TP).</p> <p>Using this tab, you can view the number of DEPI sessions for every RPD connected with the selected Cisco cBR-8 device. You can also view additional information about the remote device such as the associated tunnel IDs, L2TP class, device name, IP address, and state.</p> <p>For detailed information about each DEPI session, navigate to the Network Topology, identify the RPD, and use the RPD 360 view for detailed information such as the DEPI session modes, remote states, associated pseudowires, etc.</p>
Fiber Node Utilization	Device	Yes	<p>View the list of fiber nodes on the selected device, their streaming modes (upstream or downstream), and the average utilization of each fiber node (average of all channels associated with the fiber node).</p> <p>For a graphical representation of the percentage range of utilization mapped to the number of fiber nodes per range, view the Fiber Node Downstream/Upstream Utilization graph in the Performance tab.</p>
Mac Domain Utilization	Device	Yes	<p>View the list of MAC Domains available on the selected device, their streaming modes (upstream or downstream), and the average utilization values per Mac domain node (average of all channels associated with every Mac domain).</p> <p>For a graphical representation of the percentage range of utilization mapped to the number of mac domains per range, view the MD Downstream/Upstream SG Utilization graph in the Performance tab.</p>
Cable Controller Utilization	Line Card	Yes	<p>View the configured controller types on the selected card, their streaming modes (upstream or downstream), and the average utilization of each controller (average of the bandwidth utilized on all channels associated with the controller).</p>

## Monitor the Health of RPD to cBR-8 Links

The links between cBR-8 devices and its connected RPDs are represented with the link type L2TP in Cisco EPN Manager . To view the links in the network topology and display the associated link 360 details, see [Get More Information About Links, on page 87](#).

The table below explains the link states once cBR-8-RDPs association details are added to Cisco EPN Manager :



Icon	Status	Description
	Down	Cisco cBR-8 device to RPD association is not formed and the L2TP tunnel creation process is down.
	Online/Up	Online-Cisco cBR-8 device to RPD association is formed and the L2TP tunnel creation process is initiated. Up-Cisco cBR-8 device to RPD association is completed and the link is active.
	In Progress	The status of Cisco cBR-8 device to RPD association is being discovered.
	Deployment Pending	Cisco cBR-8 device to RPD association is not formed and hence the L2TP tunnel creation process is not initiated.

For more information about the service states icons in the Link 360 view, see [Link Serviceability States](#), on page 161.

## View the Cable Dashboard

The Cable dashboard provides an executive overview of your cable network including the important issues currently affecting your network of Cisco cBR-8 devices. To open this dashboard, choose **Dashboard > Cable**. For more information, see [Cable Dashboard Overview](#), on page 15.

## Visualize the Topology of Cable Devices on the Network Topology

When RPDs are discovered from Cisco cBR-8 devices, you can view the L2TP links and other alarm information in the topology map. You can view cable devices in the network topology in the following ways:

- Click **Maps > Topology Maps > Network Topology** in the left navigation panel.
- Click the Geographical Map icon.
- By clicking the **Geographical Map** hyperlink from the Cable RPDs Association page.

For more information on the network topology features, see [View Your Network on a Geographical Map \(Geo Map\)](#), on page 175





## PART VI

# Manage Circuits

- [Overview of Circuit/VC Discovery and Provisioning, on page 415](#)
- [Provision Circuits/VCs, on page 431](#)
- [View and Manage Discovered/Provisioned Circuits/VCs, on page 519](#)
- [Monitor and Troubleshoot Circuits/VCs, on page 551](#)





## CHAPTER 15

# Overview of Circuit/VC Discovery and Provisioning

---

- [Circuits/VCs Provisioning Overview, on page 415](#)
- [Supported Carrier Ethernet VCs , on page 416](#)
- [Supported Network Structure for Provisioning EVCs, on page 419](#)
- [Supported Optical Circuits , on page 419](#)
- [Supported Circuit Emulation Services, on page 425](#)
- [Supported L3VPN Services, on page 427](#)
- [Supported MPLS Traffic Engineering Services, on page 428](#)
- [Supported Serial Services, on page 429](#)
- [Circuit/VC Discovery Overview, on page 430](#)

## Circuits/VCs Provisioning Overview

Cisco EPN Manager supports provisioning of circuits/VCs for various technologies such as Carrier Ethernet (CE), Optical/DWDM, L3VPN, Circuit Emulation, and MPLS Traffic Engineering. Mostly, a circuit spans across multiple devices. You must make configuration changes across multiple devices to provision a circuit. Cisco EPN Manager provides a Provisioning Wizard that allows you to make the required configuration changes across multiple devices that participate in a circuit.

The Provisioning Wizard collects all the required information in a step-by-step approach and generates the required configuration for all the devices. You can review the configurations generated for each device, and then choose to either make any changes in the service parameters or deploy the configurations to the devices.

The configuration changes are deployed to the participating devices as an 'atomic' transaction. Cisco EPN Manager does a best-effort attempt to either carry out all these operations together or does none at all. To implement the concept of 'atomic' transaction, Cisco EPN Manager has the rollback feature, which helps to recover from failures during provisioning.

When configuring multiple devices, if the configuration fails in any of the devices, Cisco EPN Manager does a best-effort to rollback the configuration changes made so far in all the participating devices. The device configuration states are restored to the same state, which was there before the provisioning operation was attempted.

## Supported Carrier Ethernet VCs

In a Carrier Ethernet (CE) network, data is transported across point-to-point and multipoint-to-multipoint Ethernet Virtual Connections (EVCs) and Operator Virtual Connections (OVCs) according to the attributes and definitions of the various service types—that is, E-Line, E-LAN, E-Tree, E-Access, and EVPN Virtual Private Wire Service.

Each EVC type has a port-based service and a VLAN-based service. These are differentiated by the method for service identification used at the UNIs. EVCs using all to one bundling UNIs (port-based) are referred to as ‘Private’, while EVCs using UNIs that are service multiplexed (VLAN-based), are referred to as ‘Virtual Private’

For E-Line, E-LAN, and E-Tree services, each EVC carries data in the form of CE service frames from UNI (User Network Interface) to UNI, where the UNI is the physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber. E-Access Operator Virtual Circuits (OVCs) allow service provider interconnections at the ENNI (External Network Network Interface), which is the physical demarcation point between the responsibility of two interconnecting Service Providers.

Each EVC can be configured with a rich set of attributes that include bandwidth profiles (Committed Information Rate - CIR, Excess Information Rate - EIR, Committed Burst Size - CBS, Excess Burst Size - EBS), multiple classes of service, application-oriented performance objectives, traffic management, forwarding rules, and so on.

Cisco EPN Manager supports the discovery and provisioning of the following EVC types, which are described in these topics:

- [E-Line, on page 417](#):
  - MPLS to the edge
  - Single-segment pseudowire
  - Ethernet access—local, G.8032, ICCP-SM
- [E-LAN, on page 417](#)
  - MPLS to the edge
  - Single-segment pseudowire
  - VPLS/H-VPLS with redundant pseudowire
  - Ethernet access—VPLS-based
- [E-Tree, on page 418](#)—MPLS to the edge
- [E-Access, on page 418](#)—MPLS to the edge
- [EVPN Virtual Private Wire Service \(VPWS\), on page 419](#)—Provisioning is not supported in Cisco EPN Manager for this service type.

## Core Technology for Multipoint EVCs

The core technology for the E-LAN or E-Tree EVC can be either VPLS (Virtual Private LAN Services) or H-VPLS (Hierarchical VPLS).

- VPLS—A Layer 2 VPN technology that provides Ethernet-based multipoint-to-multipoint communication over MPLS networks. VPLS allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. The network emulates a LAN switch or bridge by connecting customer LAN segments to create a single bridged Ethernet LAN.

- **H-VPLS**— Partitions the network into several edge domains that are interconnected using an MPLS core. The edge devices learn only of their local U-PE devices and therefore do not need large routing table support. The H-VPLS architecture provides a flexible architectural model that enables Ethernet multipoint and point-to-point Layer 2 VPN services, as well as Ethernet access to Layer3 VPN services, enabling service providers to offer multiple services across a single high-speed architecture.

In E-TREE EVCs, H-VPLS supports redundancy. Two hubs operate as connectors through which all traffic passes. If the primary hub fails, traffic is switched to the backup hub. With H-VPLS as the core technology, there is no direct connection between the E-tree root and leaf. H-VPLS is used together with split-horizon capabilities to prevent leaf to leaf communication.

If VPLS is used as the core technology, redundancy is not supported and there is a direct connection between root and leaves. The hub is located in the root, meaning that the root assumes the role of the hub.

## E-Line

E-Line refers to an Ethernet service that is based on a point-to-point EVC. There are two types of E-Line VCs:

- **Ethernet Private Line (EPL)**, which has the following characteristics:
  - Port-based
  - Uses a point-to-point EVC between two UNIs to provide a high degree of transparency such that service frames, headers, and most Layer 2 protocols are identical at both the source and destination UNI.
  - All to one bundling where all CE-VLAN IDs are bundled to one EVC. No service multiplexing.
- **Ethernet Virtual Private Line (EVPL)**, which has the following characteristics:
  - VLAN-based
  - Uses a point-to-point EVC between two UNIs, but does not provide full transparency as with the EPL, that is, all Layer 2 control protocols are discarded at the UNI.
  - Allows for service multiplexing, which means that more than one EVC can be supported at the UNI.

## E-LAN

E-LAN refers to an Ethernet service that is based on a multipoint-to-multipoint EVC. There are two types of E-LAN VCs:

- **Ethernet Private LAN (EP-LAN)**, which has the following characteristics:
  - Port-based
  - All-to-one bundling at the UNI
  - Very transparent, no manipulation of CE-VLAN IDs and PCP bits
  - EP-LAN multiport transparency is more complex than EPL
- **Ethernet Virtual Private LAN (EVP-LAN)**, which has the following characteristics:
  - VLAN-based
  - Allows for service multiplexing and bundling

## E-Tree

An E-Tree VC is a rooted multipoint VC that connects a number of UNIs providing sites with hub and spoke multipoint connectivity. Each UNI is designated as either *root* or *leaf*. A root UNI can communicate with any leaf UNI. A leaf UNI can communicate only with a root UNI, not with another leaf UNI.

E-Tree VCs provide the separation between UNIs required to deliver a single service instance in which different customers (each having a leaf UNI) connect to an ISP which has one or more root UNIs. Having more than one root UNI is useful for load sharing and resiliency schemes.

There are two types of E-Tree VCs:

- Ethernet Private TREE (EP-TREE), which has the following characteristics:
  - Rooted multipoint, port-based.
  - All-to-one bundling at the UNI.
  - Simpler than typical hub and spoke configuration using multiple EPLs. Hub function is performed by the root UNI.
  - Provides CE-VLAN tag preservation and tunneling of key Layer 2 Control Protocols.
  - Supports CE-VLAN CoS preservation.
- Ethernet Virtual Private TREE (EVP-TREE), which has the following characteristics:
  - Rooted multipoint, VLAN-based.
  - Provides an alternative to multiple EVPLs multiplexed at the hub site.
  - Used in cases where one or more of the subscriber's UNIs also supports other services, e.g., EVPL or EVP-LAN.

## E-Access

An Ethernet Access service allows a service provider to construct an Operator Virtual Connection (OVC) between two customer sites where one of the sites is located outside of the service provider's own network. In such cases a service provider uses an E-Access service offered by a local wholesale access provider to reach the out-of-franchise UNI. The service provider connects to the E-Access service at an ENNI, and traffic is forwarded between the ENNI and the out-of-franchise UNI across an Operator Virtual Connection (OVC).

E-Access definitions include attributes related to the external interfaces, in this case, the ENNI and the UNI, as well as attributes related to the virtual Ethernet connection associating these external interfaces. E-Access services use a point-to-point OVC to associate one OVC endpoint at an ENNI and one OVC endpoint at a UNI.

There are two types of E-Access VCs:

- Access EPL, which has the following characteristics:
  - Private or port-based
  - One OVC per UNI
  - All CE-VLAN IDs are mapped to the OVC
- Access EVPL, which has the following characteristics:
  - VLAN-based
  - Can be multiple OVCs per UNI
  - Multiple but not all CE-VLAN IDs are bundled to one OVC



## EVPN Virtual Private Wire Service (VPWS)

The EVPN-VPWS is a BGP control plane solution for point-to-point services. It implements the signaling and encapsulation techniques for establishing an EVPN instance between a pair of PEs. It has the ability to forward traffic from one network to another without MAC lookup. The use of EVPN for VPWS eliminates the need for signaling single-segment and multi-segment PWs for point-to-point Ethernet services. The EVPN-VPWS technology works on IP / MPLS core; IPcore to support BGP and MPLS core for switching packets between the endpoints.

**Note**

Cisco EPN Manager supports only the discovery of single-homing EVPN-VPWS services and does not support the provisioning for this type of services.

## Supported Network Structure for Provisioning EVCs

Cisco EPN Manager can provision EVCs and OVCs over a mix of access networks. The endpoints can be configured directly on an MPLS router, an Ethernet Access switch, or an nV satellite attached to a Cisco ASR 9000 router. The EVCs may have endpoints in different Ethernet Access networks, in the same network, or on the same device. Cisco EPN Manager will configure as much as is needed to create the connectivity.

EVCs can be provisioned over the following networks:

- **MPLS Domain**—Cisco EPN Manager assumes that the managed network contains a single MPLS domain. Any router can communicate with any other router via a targeted LDP session. Alternatively MPLS end-to-end connectivity can be achieved using MPLS Traffic Engineering or segment routing.
- **Ethernet Access Network**—Cisco EPN Manager supports EVC provisioning over Ethernet Access networks attached to a central MPLS domain. The networks are discovered by the system. EVCs can be provisioned over a G.8032 access ring or over ICCP-SM links. The access network can be:
  - A G.8032 ring. This should include a router to enable the creation of EVCs that cross the MPLS domain.
  - A G.8032 open ring, which means a sequence of links.
- **Cisco ASR 9000 nV Satellite Topology**—Cisco EPN Manager can configure EVCs on single-homed nV satellite devices attached to an Cisco ASR 9000 host.

To support service discovery and provisioning, Cisco EPN Manager must discover the topology in the access network. For successful discovery, the following prerequisites must be fulfilled:

- For ICCP-SM, LAG must be configured with LACP.
- For G.8032, CDP or LLDP must be configured on the ring ports.

## Supported Optical Circuits

A circuit represents an end-to-end connection between two or more connection termination points (CTPs). A circuit consists of an alternating series of cross-connections and link connections. In its simplest form, a circuit consists of a single cross-connection (if the circuit is defined between two CTPs on the same NE). A circuit can be bidirectional or unidirectional, point-to-point or point-to-multipoint, and protected or unprotected.

ess supports the provisioning of Dense Wavelength Division Multiplexing (DWDM) optical channel (OCH) circuit types and Optical Transport Network (OTN) circuit types. The DWDM optical technology is used to increase bandwidth over existing fiber optic backbones. It combines and transmits multiple signals simultaneously at different wavelengths on the same fiber. In effect, one fiber is transformed into multiple virtual fibers.

Cisco EPN Manager supports the following optical circuits types:

- [Dense Wavelength Division Multiplexing \(DWDM\) Circuits, on page 420](#)
  - [Optical Channel Network Connection \(OCHNC\) WSON, on page 420](#)
  - [Optical Channel Client Connection \(OCHCC\) WSON, on page 420](#)
  - [Optical Channel \(OCH\) Trail WSON, on page 421](#)
  - [Optical Channel \(OCH\) Trail Connecting NCS 1002, NCS 55xx, and ASR 9K Devices, on page 421](#)
  - [Optical Channel \(OCH\) Trail User-to-Network Interface \(UNI\), on page 422](#)
  - [Spectrum Switched Optical Network \(SSON\) Circuits, on page 422](#)
- [Optical Transport Network \(OTN\) Circuit, on page 423](#)
  - [Optical Channel Data Unit User-to-Network Interface \(ODU UNI\), on page 424](#)
  - [Optical Channel Data Unit \(ODU\) Tunnel, on page 424](#)
  - [Optical Channel Payload Unit \(OPU\) Over Optical Channel Data Unit \(ODU\), on page 425](#)
  - [Optical Channel Data Unit User-to-Network Interface \(ODU UNI\) Hairpin, on page 425](#)
  - [Optical Channel Data Unit \(ODU\), on page 425](#)

## Dense Wavelength Division Multiplexing (DWDM) Circuits

The following topics describe the different optical channel (OCH) and media channel (MCH) circuit types.

### Optical Channel Network Connection (OCHNC) WSON

OCHNC WSON circuits establish connectivity between two optical nodes on a specified C-band wavelength. The connection is made through the ports present on the wavelength selective switches, multiplexers, demultiplexer, and add/drop cards. In an OCHNC WSON circuit, the wavelength from a source OCH port ingresses to a DWDM system and then egresses from the DWDM system to the destination OCH port.

### Optical Channel Client Connection (OCHCC) WSON

OCHCC WSON circuits extend the OCHNC WSON to create an optical connection from the source client port to the destination client port of the TXP/MXP cards. An OCHCC WSON circuit represents the actual end-to-end client service passing through the DWDM system. Each OCHCC WSON circuit is associated to a pair of client or trunk ports on the transponder (TXP), muxponder (MXP), GE\_XP (in layer-1 DWDM mode), 10GE\_XP (in layer-1 DWDM mode), or ITU-T line card. The OCHCC WSON circuits can manage splitter protection as a single protected circuit. However, for the Y-Cable protection, two OCHCC WSON circuits and two protection groups are required.



---

**Note** Cisco EPN Manager can discover the LMP links between a Cisco NCS 2000 series device and a Cisco IOS-XR device that are connected by an OCHCC WSON circuit.

---

## Optical Channel (OCH) Trail WSON

OCH trail WSON circuits transport the OCHCC WSON circuits. The OCH trail WSON circuit creates an optical connection from the source trunk port to the destination trunk port of the Transponder (TXP), Muxponder (MXP), GE\_XP, 10GE\_XP, or ITU-T line card. The OCH trail WSON represents the common connection between the two cards, over which all the client OCHCC WSON circuits, SVLAN circuits or STS circuits are carried. Once an OCHCC WSON is created, a corresponding OCH Trail is automatically created. If the OCHCC WSON is created between two TXP, MXP, GE\_XP, or 10GE\_XP cards, two circuits are created in the CTC. These are:

- One OCHCC WSON (at client port endpoints)
- One OCH trail WSON (at trunk port endpoints)

If the OCHCC WSON is created between two TXPP or two MXPP cards, three circuits are created in the CTC. These are:

- One OCHCC WSON (at client port endpoints)
- Two OCH Trails WSON (at trunk port endpoints). One for the working and other for the protect trunk.

## Optical Channel (OCH) Trail Connecting NCS 1002, NCS 55xx, and ASR 9K Devices

Cisco EPN Manager can discover an OCH Trail circuit from the following devices:

- Source trunk port of an NCS 1002 device to the destination trunk port of another NCS 1002 device.
- Source trunk port of an NCS 55xx device (trunk ports on NCS55-6X200-DWDM-S card) to the destination trunk port of another NCS 55xx device.
- Source trunk port of an ASR 9K device (trunk port on ASR9K-400G-DWDM-TR) to the destination trunk port of another ASR 9K device.

The trunk port of each of these devices must be connected via a manual link to the passive units of NCS 2K devices. Where the manual links are terminated, an OCH-NC circuit must be created as a pre-requisite between the ports of the passive units of NCS 2K network.



---

**Note** Provisioning is not supported for this type of optical circuits.

---

## Optical Channel (OCH) Trail Hybrid Circuits

An OCH Trail hybrid circuit connects a Cisco IOS-XR device and a Cisco NCS 2000 series device. Cisco EPN Manager can discover such circuits whose trunk ports must be connected via either a manual link or an LMP link to the passive units of Cisco NCS 2000 series devices.



---

**Note** Provisioning is not supported for this type of optical circuits.

---

## Optical Channel (OCH) Trail User-to-Network Interface (UNI)

An OCH trail UNI circuit establishes connectivity between the following devices:

- Cisco NCS 2000 series devices and Cisco NCS 4000 series devices. It provides an end-to-end configuration of DWDM network that consists of Cisco NCS 2000 series devices and terminates on a Cisco NCS 4000 series device. When an OCH trail UNI circuit is created in a Cisco NCS 4016 network element, a corresponding OCHNC circuit is created in the Cisco NCS 2006 network element.




---

**Note** You will not be able to modify or delete the OCHNC circuit.

---

- Cisco NCS 1000 series devices that act as UNI-C and Cisco NCS 2000 series devices that act as UNI-N. The OCH trail UNI circuit originates from an NCS 1002 trunk interface (UNI-C) on the source NCS 1002 node and terminates on the NCS 2000 series interface (UNI-N) on the destination NCS 2000 series node to create an optical connection. The prerequisite for the OCH trail UNI circuit is to create a Link Management Protocol (LMP) link between the optical channel Add/Drop NCS 2000 series interface on the NCS 2000 series node and the NCS 1002 interface on the NCS 1002 node. See [Configure GMPLS and WSON Properties, on page 329](#).




---

**Note** Cisco EPN Manager discovers the OCH Trail UNI circuits that originates from NCS 1002 device running on software version 6.3.2.

---

The LMP link can either be a numbered link or an unnumbered link. An unnumbered link does not have an IP address.

- For unnumbered links, Cisco EPN Manager creates the required explicit path object on the NCS 1000 series device, which is the source device. This device will contain two constraints, one for the source peer NCS 2000 series device and the other for the destination device. You can add more constraints as required.
- For numbered links, a default explicit path object is not required. If you want to add constraints, you must first specify the source NCS 2000 series node in the explicit path even if the node is selected as the source endpoint of the OCH Trail UNI circuit. If you do not add the source NCS 2000 series node as your first constraint, the corresponding OCHNC circuit on the NCS 2000 series node will not be created.




---

**Note** You cannot use both numbered and unnumbered links for the same OCH Trail UNI circuit.

---

## Spectrum Switched Optical Network (SSON) Circuits

SSON circuits allow you to provide more than 96 channels in a span. Using the SSON functionality, the circuits are placed closer to each other if they are created within a media channel group. The minimum spacing between circuits is 50 GHz.

SSON circuits can be created only if the source and destination nodes have the SSON package installed.



**Note** The existing OCHNC, OCHCC, and OCH Trail circuits cannot be upgraded to SSON circuits.

Cisco EPN Manager supports the following SSON circuits:

- **Media Channel Circuits**—Media channel (MCH) works on any available frequency (flexible frequency) and establishes connection between two optical nodes. A continuous section of the spectrum is allocated between the source and destination nodes. The MCH contains information regarding the allocated optical bandwidth. A media channel can be of three modes:
  - **Media Channel Trail**—MCH trail SSON circuits transport the MCHCC SSON circuits. These circuits create optical connection between trunk ports of a co-located TXP (based on the carrier trails).
  - **Media Channel Network Connection (MCHNC)**—MCHNC SSON circuits create optical connection between filter ports (based on the carrier).
  - **Media Channel Client Connection (MCHCC)**—MCHCC circuits create optical connection between client ports of a co-located TXP.
- **Media Channel Group (MCHG)**—MCHG is a container that can include one or more media channels. Media channels are grouped together to increase the spectral efficiency. Circuits can be created at closer intervals, when compared to OCH circuits. Maximum number of media channels can be achieved on a single fiber, if the MCHG covers the entire C-band.

## Optical Transport Network (OTN) Circuit

OTN specifies a digital wrapper, which is a method of encapsulating an existing frame of data, regardless of the native protocol, to create an optical data unit (ODU), similar to that used in SDH/SONET. OTN provides the network management functionality of SDH/SONET, but on a wavelength basis. A digital wrapper, however, is flexible in terms of frame size and allows multiple existing frames of data to be wrapped together into a single entity that can be more efficiently managed through a lesser amount of overhead in a multi-wavelength system.

The OTN specification includes framing conventions, non-intrusive performance monitoring, error correction (FEC), rate adaption, multiplexing mechanisms, ring protection, and network restoration mechanisms operating on a wavelength basis.

A key element of a digital wrapper is the forward error correction (FEC) mechanism that provides performance gains for improved margins and extended optical reach.

The OTN architecture is compliant to ITU-T G.872. An OTN circuit can be established statically or dynamically between ingress and egress nodes using Resource Reservation Protocol (RSVP) signaling. An OTN circuit is established and maintained as a label switched path (LSP) between the ingress and egress Label Switched Routers (LSRs) switched through transit LSRs. An LSP can be established as a soft permanent connection (SPC) when the request comes from the user interface.

Following are the types of OTN circuits:

- [Optical Channel Data Unit User-to-Network Interface \(ODU UNI\), on page 424](#)
- [Optical Channel Data Unit \(ODU\) Tunnel, on page 424](#)
- [Optical Channel Payload Unit \(OPU\) Over Optical Channel Data Unit \(ODU\), on page 425](#)
- [Optical Channel Data Unit User-to-Network Interface \(ODU UNI\) Hairpin, on page 425](#)

- [Optical Channel Data Unit \(ODU\), on page 425](#)

## Optical Channel Data Unit User-to-Network Interface (ODU UNI)

ODU is the transport container defined to carry client signals from network ingress to egress. The ODU provides a payload area for client data along with performance monitoring and fault management. The payload area of an ODU may contain a single non-OTN signal as a client or may contain multiple lower rate ODUs as clients. An ODU UNI circuit represents the actual end-to-end client service passing through the OTN architecture.

### Open Ended ODU UNI

In an open-ended ODU UNI circuit, one or both end points may be connected to ODU subcontrollers, instead of client payload controllers.

Cisco EPN Manager supports three types of open-ended ODU UNIs:

- Only the source interface is an ODU subcontroller
- Only the destination interface is an ODU subcontroller
- Both source and destination interfaces are ODU subcontrollers

To create an open-ended ODU UNI circuit, you must configure ODU subcontrollers on devices before adding the devices to Cisco EPN Manager. Use the **controller oduk** command to configure ODU subcontrollers on devices.

### Example: Configure an ODU subcontroller on a Cisco NCS 4000 Device

In this example, two ODU0 subcontrollers are configured to an ODU1 controller.

```
RP/0/RP0:router#conf
RP/0/RP0:router(config)# controller ODU10/1/0/1
RP/0/RP0:router(config-odul)# tsg 1.25G
RP/0/RP0:router(config-odul)# ODU0 tpn 1 ts 1
RP/0/RP0:router(config-odul)# ODU0 tpn 2 ts 2
RP/0/RP0:router(config-odul)#commit
```

To verify that the ODU subcontrollers are configured correctly on the device:

```
RP/0/RP0:router#sh controllers ODU0 ?
0/1/0/0      ODU0 Interface Instance
0/1/0/1/10   ODU0 Interface Instance
0/1/0/1/20   ODU0 Interface Instance
R/S/I/P      Forward interface in Rack/Slot/Instance/Port format
```

After configuring the ODU subcontrollers on the device, you must add the device to Cisco EPN Manager. You can then verify that the ODU0 0/1/0/1/10 and ODU0 0/1/0/1/20 subcontrollers are available in the inventory.

## Optical Channel Data Unit (ODU) Tunnel

ODU tunnel circuits transport the ODU UNIs. The ODU tunnel represents the common connection between two Cisco NCS 4000 series devices that are connected with Traffic Engineering (TE) links. Once an ODU UNI circuit is created, a corresponding ODU tunnel is automatically created.

## Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU)

OPU over ODU circuits provide a high-bandwidth point-to-point connection between two customer designated premises. Client signals are mapped over an OTN framing structure with in-band management through GCC0. These circuits use ODU UNI circuits to carry client signals through the network. You need to perform the following tasks to create and provision an OPU over ODU circuit:

- Using Cisco EPN Manager, create an ODU UNI circuit. For information about how to create ODU UNI circuits, see [Create and Provision an OTN Circuit, on page 460](#).
- Using Cisco Transport Controller (CTC), create LMP links and enable the links on the devices that you want to use in the OPU over ODU circuits. For information about how to create LMP, see the "DLP-K27 Create an LMP Using CTC" section in the [OTN and DWDM Configuration Guide for Cisco NCS 4000 Series](#).
- Using Cisco EPN Manager, create an OPU over ODU circuit with the LMP links enabled devices. For information about how to create OPU over ODU circuits, see [Create and Provision an OTN Circuit, on page 460](#).

## Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin

An ODU UNI Hairpin circuit is similar to an ODU UNI circuit, but it is created in the management plane and it is an intra node circuit, that is, the source and destination is the same device but with different interfaces. In this type of circuit, the connection is established between two clients or two ODU subcontrollers.

Cisco EPN Manager supports the following types of ODU UNI Hairpin circuits:

- Circuits without open-ended cross-connect—In this type of circuits, the interfaces of both source and destination are not OTU interfaces.
- Circuits with open-ended cross-connect on one side—In this type of circuits, the interface of either source or destination is an OTU interface.
- Circuits with open-ended cross-connect on both sides—In this type of circuits, the interface of both source or destination are OTU interfaces.

## Optical Channel Data Unit (ODU)

The Optical Channel Data Unit (ODU) circuit represents the common connection between two Cisco NCS 2000 series devices that are connected with Traffic Engineering (TE) links. The ODU is created as a sub controller of an OTU controller. ODU contains information for the maintenance and operational functions to support optical channels. ODU Over Head (OH) information is added to the ODU payload to create the complete ODUk. The ODUk OH consists of portions dedicated to the end-to-end ODUk path and to six levels of tandem connection monitoring. The ODUk path OH is terminated where the ODUk is assembled and disassembled. The TCM OH is added and terminated at the source and sink to the corresponding tandem connections.

ODU cross connection is an end-to-end channel between two OTN or client ports in the OTN network. Cisco EPN Manager supports ODU cross connections with bidirectional SNC-N protection.

## Supported Circuit Emulation Services

Circuit Emulation (CEM) provides a protocol-independent transport over IP networks. It enables proprietary or legacy applications to be carried transparently to the destination, similar to a leased line. In traditional TDM

networks, numerous physical circuits are maintained between geographically diverse locations to provide TDM transport. CEM allows TDM endpoints to connect across an IP/MPLS core. In CEM, endpoints are connected to the TDM circuits, but the circuits terminate at each local router that has the IP/MPLS connectivity available. The router then transports those TDM frames across the IP/MPLS core via Circuit Emulation (CEM) pseudowires (PWs) to the remote endpoint that also has the IP/MPLS connectivity available. Thus, the TDM endpoints can communicate as if they were directly connected by physical circuits.

Cisco EPN Manager supports the following CEM modes:

- **Structure-Agnostic time-division multiplexing (TDM) over Packet (SAToP)**—This is the unstructured mode in which the incoming TDM data is considered as an arbitrary bit stream. It disregards any structure that may be imposed on the bit stream. SAToP encapsulates the TDM bit streams as pseudowire (PWs) over PSN.
- **Circuit Emulation over Packet (CEP)**—This mode is used to emulate Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) circuits and services over MPLS. To transport SONET/SDH circuits through a packet-oriented network, the Synchronous Payload Envelope (SPE) or Virtual Tributary (VT) is broken into fragments. A CEP header and optionally an RTP header are prepended to each fragment.
- **Circuit Emulation Service over Packet Switched Network (CESoPSN)**—This is the structured mode in which the structured TDM signals are encapsulated as PWs and transmitted over PSN. It selects only valid timeslots and disregards the idle timeslots for transmission. Thus, CESoPSN can save utilized bandwidth.

Cisco EPN Manager supports the following CEM service types depending on the rate at which the circuits can transmit data:

- **DS0**—A basic digital signal with transmission data rate of up to 64 Kbps.




---

**Note** Cisco NCS 42XX series devices does not support the DS0 service type.

---

- **T1 and E1**—Digital Signal (DS) is known as T-carrier in North America, South Korea, and Japan and as E-carrier in the rest of the world. The T1 circuit has a transmission data rate of up to 1.544 Mbps. The E1 circuit has a transmission data rate of up to 1.984 Mbps in framed mode and 2.048 Mbps in unframed mode.
- **T3 and E3**—The T3 circuit has a transmission data rate of up to 44.736 Mbps. The E3 circuit has a transmission data rate of up to 34.368 Mbps. The T3 or E3 circuit can transport 672 DS0 level channels and 28 DS1 level channels within its payload.
- **VT 1.5**—A virtual tributary network line with transmission data rate of up to 1.728 Mbps.
- **STS1**—A synchronous transport signal with transmission data rate of up to 51.84 Mbps.
- **STS3**—A synchronous transport signal with transmission data rate of up to 155.52 Mbps.
- **STS12**—A synchronous transport signal with transmission data rate of up to 622.08 Mbps.
- **STS48**—A synchronous transport signal with transmission data rate of up to 2488.32 Mbps.
- **X.21**—The X.21 interface supports the serial data speed that are multiples of 64 Kbps. The maximum limit of speed can be 2048 Kbps. The pseudowire utilizes Circuit Emulation Service over Packet-Switched Network (CESoPSN) in E1 mode to transport the X.21 traffic over the MPLS network.
- **C37.94**—The C37.94 is an IEEE standard that defines the communication of protection relays with communication equipment using optical fibers. This interface supports pseudowire that utilizes CESoPSN to transmit data. The frame format defined for the C37.94 interface is used to transmit data in packet format from the multiplexer to the tele-protection equipment and from the tele-protection equipment to the multiplexer equipment. The IEEE defines the C37.94 standard as  $N * 64$  kbps optical fiber interface



to provide transparent communications between tele-protection relays and multiplexers equipments. The C37.94 standard describes the interconnection details for the variable N, (where  $N = 1, 2 \dots 12$ ), which describes a multiple of 64 kilobit per second connections at which the communication link is to operate.

- **EM-Voice**—The E&M interface supports pseudowire types that utilize CEM transport, CESoPSN in T1 and E1 modes to transport analog signals and voice traffic over MPLS. The voice port interfaces that connect the device to E & M lines pass voice data and signaling between the packet network and the analog-circuit-switched network. The devices in the packet network must be configured to convey signaling information in a way that the circuit-switched network can understand. The devices must also be able to understand signaling information received from the circuit-switched network. E&M signaling interface uses special signaling paths that are separate from the trunk circuit's audio path to convey information about the calls.

## Supported L3VPN Services

An MPLS Layer 3 VPN creates a private IP network. The customer connects to the network via customer edge (CE) routers, which act as IP peers of provider edge (PE) routers.

### Virtual Routing and Forwarding (VRFs)

On the PE, Virtual Routing and Forwarding (VRF) instances act as virtual IP routers dedicated to forwarding traffic for the L3VPN service. The VRFs learn the routes to each other via the Multi-Protocol Border Gateway Protocol (MP-BGP), and then forward traffic using MPLS.

A VPN is comprised of at least one but typically several VRFs. Cisco EPN Manager uses the VPN ID to discover which VRFs together form a single VPN. If Cisco EPN Manager discovers an existing network where no VPN ID has been provisioned, it takes all VRFs with the same name and associates them into one VPN. For VPNs created using Cisco Prime Provisioning, which uses a naming convention with version number prefixes and different suffixes, Cisco EPN Manager will recognize the different VRFs as belonging to one VPN.

In general there is a regular expression which can be configured to allow for varying naming convention.

### Route Targets (RTs)

The connections between VRFs are defined using Route Targets (RTs) that are imported and exported by the VRFs. Cisco EPN Manager makes it easy to set up a full mesh of connections, and automatically allocates the route target to be used. The route target consists of a prefix which is either an AS number or an IPv4 address, for example, a full mesh prefix, 100 [681682]. The prefix can be selected from the existing BGP autonomous system (AS) numbers in the network, or it can be entered manually. The second number following the prefix is allocated automatically by Cisco EPN Manager.

Alternatively or in addition to the full mesh, it is possible to manually select route targets. During VPN creation, there is an initial screen where you type in the route targets to be used within a VPN, and then for each VRF you can select which route targets you import and export. You also specify for which address family (IPv4 or IPv6) you will use the route target. This can be used for example to configure extranets, by importing route targets used in other VPNs.

### Route Redistribution

The routes that are exchanged between the PE and the CE have to be redistributed into the MP-BGP routing protocol so that remote endpoints can know which prefixes can be reached at each VRF. To control route redistribution, Cisco EPN Manager allows you to define the required protocol (Static, Connected, or RIP), the protocol's metric value, and optionally the applicable route policy.

### Endpoints

Cisco EPN Manager supports the creation of IP endpoints on Ethernet subinterfaces. It supports selecting untagged encapsulation, or specifying an outer and optionally an inner VLAN, with 802.1q or 802.1ad encapsulation. You can specify both IPv4 and Ipv6 addresses at an endpoint. You can also specify the BGP and OSPF neighbor details to provision BGP and OSPF neighbors between CE and PE.

For information on how to provision L3VPN service using Cisco EPN Manager, see, [Provision L3VPN Services, on page 467](#).

## Supported MPLS Traffic Engineering Services

In traditional IP networks, packets are forwarded on a per-hop basis where a route lookup is performed on each router from source to destination. The destination-based forwarding mechanism leads to suboptimal use of available bandwidth between a pair of routers in the network. Mostly, the suboptimal paths are under-utilized in IP networks. To avoid packet drops due to inefficient use of available bandwidth and to provide better performance, traffic engineering (TE) is implemented. TE directs the traffic that is destined to follow the optimal path to a suboptimal path, thus enabling better bandwidth utilization between a pair of routers.

Multiprotocol Label Switching (MPLS) is an integration of Layer 2 and Layer 3 technologies. In an MPLS domain, unique labels are assigned to data packets and the packets are forwarded based on these labels. It avoids the complex lookup in a routing table. MPLS creates a VC switching function to provide similar performance on the IP-based network services as compared to those delivered over traditional networks such as Frame Relay or Asynchronous Transfer Mode (ATM).

By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. MPLS TE enables an MPLS backbone to replicate and expand the TE capabilities of Layer 2 over Layer 3.

MPLS TE uses Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP) across the backbone. The path that an LSP uses is based on the LSP resource requirements and network resources, such as bandwidth and link attributes. Available resources are flooded by means of extensions to a link-state-based Interior Gateway Protocol (IGP). Cisco EPN Manager supports OSPF as the IGP to flood the available bandwidth and link status information across the network. Based on this information, the ingress (headend) router gathers information on all the available resources in the network along with the topology to define tunnels through the network between a set of MPLS-enabled routers. This is called as constraint-based routing. When a shortest path is over-utilized, the IGP automatically routes the traffic to these LSPs. You can also provision explicit paths for MPLS TE tunnels.

Cisco EPN Manager provides full path protection mechanism for MPLS TE tunnels against path, link, and node failures. A secondary LSP is established to provide failure protection for the protected LSP that is carrying a tunnel's TE traffic. When there is a failure on the protected LSP, the source router immediately enables the secondary LSP to temporarily carry the tunnel's traffic. If there is a failure on the secondary LSP, the tunnel no longer has path protection until the failure along the secondary path is cleared.

Cisco EPN Manager supports the following MPLS TE service types:

- [Unidirectional TE Tunnel, on page 428](#)
- [Bidirectional TE Tunnel, on page 429](#)
- [Layer 3 Link, on page 429](#)

## Unidirectional TE Tunnel

MPLS TE tunnels are unidirectional tunnels that connect a pair of LSRs. Once the unidirectional tunnel is created, a label is assigned for the tunnel that corresponds to a specific path in a MPLS network. The traffic

is routed through the tunnel. You must create another unidirectional tunnel between the same routers to route the return traffic. For example, router A is the head end and router B is the tail end of tunnel 1, which is a unidirectional tunnel. You must create another unidirectional tunnel, say tunnel 2 with router B as the head end and router A as the tail end.

## Bidirectional TE Tunnel

Two unidirectional TE tunnels established between a pair of LSRs that are connected to each other, can be bound together to form a bidirectional co-routed TE tunnel. The binding of unidirectional tunnels is based on the source and destination addresses, global ID, association ID, and association address of the tunnels. For example, router A and router B that are connected by two unidirectional tunnels, tunnel C and tunnel D, can be bound together to form a bidirectional TE tunnel only if the following conditions are met:

- The source address of tunnel C is the destination address of tunnel D and vice versa.
- The global ID, association ID, and association address of tunnel C and D are the same. The association ID and association address for the tunnels are system-defined and you need to assign a global ID for the tunnels.

Bidirectional TE tunnels inherit the security features of RSVP-TE.

## Layer 3 Link

To enable traffic engineering links between two devices, you need to configure the following on both ends of the devices:

- Loopback interface
- Ethernet interface
- BDI Interface
- OSPF, RSVP, and MPLS
- IS-IS and BGP

You can perform these configurations using the Layer 3 link provisioning feature in Cisco EPN Manager .

## Supported Serial Services

In a serial communication, the serial port sends and receives bytes of information one bit at a time. The serial communication can be used over longer distances. The cabling between devices can extend up to 1200 meters. Serial communication is used to transmit ASCII data. Communication is completed using three transmission lines—ground, transmit, and receive. Since serial is asynchronous, the port is able to transmit data on one line while receiving data on another. Other lines are available for handshaking, but are not required.

Cisco EPN Manager supports the following serial service types:

- RS232—is a standard communication protocol that links devices in a network to allow serial data exchange. It defines the voltage for the path used for data exchange between the devices. It specifies common voltage, signal level, common pin wire configuration, and minimum amount of control signals. The RS232 interface is suitable for short-distance and low-speed requirements.

- RS485—is an EIA/TIA standard that defines a communication bus that is used to form simple networks of multiple devices. The RS485 interface can be used in simplex or half-duplex modes with a single-pair cable. Full-duplex or simultaneous transmit and receive operations can be implemented with a two-pair cable. This interface is used for high speed over long distances.
- Raw Socket—is a method for transporting serial data through an IP network. Raw Socket transports Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). Raw Socket supports point-to-point and point-to-multipoint connections. Raw Socket supports point-to-multipoint connection over an asynchronous serial line and has a built-in auto TCP connection retry mechanism.

## Circuit/VC Discovery Overview

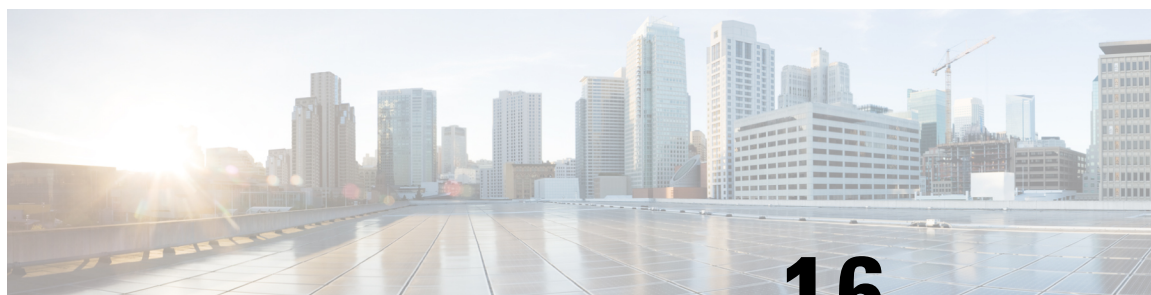
Cisco EPN Manager uses the Service Discovery feature to automatically discover circuits/VCs existing in the network. Ensure that the Service Discovery feature is enabled under **Administration > System Settings**. See [Enable and Disable Service Discovery, on page 519](#).

Circuit/VC discovery depends on device-level inventory discovery, and consists of two parts:

- Resource facing service (RFS) discovery—The RFS represents the relations between resources on different devices. During RFS discovery, the system creates device-level objects and network-level objects. Device-level RFS objects represent the circuit/VC configuration parts of the device-level configuration. Network-level RFS objects aggregate device or other network-level objects to represent network-level entities.
- Customer facing service (CFS) matching—The CFS represents the customer facing data for a circuit/VC. The CFS is derived from discovered RFS and represents the endpoints of the circuit/VC in the network. During CFS discovery, the system creates CFS objects for the discovered RFS objects.

Discovery is an ongoing process in Cisco EPN Manager. When you first start using Cisco EPN Manager, the circuits/VCs that exist in the network are discovered. Later, when you start provisioning circuits/VCs using the Provisioning Wizard, Cisco EPN Manager will discover the provisioned circuits/VCs and will search for a match between the resources used in the circuit/VC and the resources discovered from the network. When a match is found between a discovered circuit/VC and a provisioned circuit/VC, information from the provisioned CFS is copied into the discovered CFS.

Cisco EPN Manager allows you to compare between the provisioned and discovered versions to identify changes that might have been made in the device configurations and you can do a reconciliation, if necessary. See [Compare and Reconcile Provisioned and Discovered Versions of a Circuit/VC, on page 543](#)



## CHAPTER 16

# Provision Circuits/VCs

---

- Provision Circuits/VCs in Cisco EPN Manager , on page 431
- Provision EVCs in a Carrier Ethernet Network, on page 436
- Provision Circuits in an Optical/DWDM Network, on page 447
- Provision L3VPN Services, on page 467
- Provision Circuit Emulation Services, on page 483
- Provision MPLS Traffic Engineering Services, on page 489
- Provision Serial Services, on page 503
- Create Circuit/VC Profiles , on page 509
- Create QoS Profiles, on page 510
- Create Customers, on page 511
- Provision a Circuit/VC with an Unmanaged Endpoint, on page 511
- Extend a Circuit/VC Using Templates, on page 512
- Example Configuration: Extend a Circuit/VC Using CLI Templates, on page 513

## Provision Circuits/VCs in Cisco EPN Manager

The process of creating and provisioning a circuit/VC is similar for all the supported technologies and involves:

- Specifying the endpoints of the circuit/VC.
- Defining the configuration parameters of the circuit/VC.

For a detailed overview of the provisioning support in Cisco EPN Manager , see [Provision Circuits/VCs, on page 431](#).


To create and provision a new circuit/VC:

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click on the **Device Groups** button, select the required device group(s) and click **Load**.
- Step 3** Close the **Device Groups** popup window.
- Step 4** In the **Network Topology** window, click the **Circuits/VCs** tab.
- Step 5** Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

**Note** You can also access the Provisioning wizard by choosing **Configuration > Network > Service Provisioning**

- Step 6** From the **Technology** drop-down list, choose the required technology. For example, if you are creating a circuit for Optical/DWDM network, choose **Optical**.
- Step 7** In the **Service Type** area, choose the type of circuit/VC you want to create. For example, if you are creating a circuit/VC for Optical/DWDM network, the various circuit types include OCHNC WSON, OCHCC WSON, OCH-Trail WSON, OCH-Trail UNI, ODU UNI, ODU Tunnel and OPU over ODU.
- Step 8** If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles](#) , on page 509.
- Step 9** Click **Next** to go to the Customer Service Details page.
- Step 10** (Optional) Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then go to the Provisioning Wizard to start provisioning the circuit/VC.
- Step 11** Enter the service name and its description.
- Step 12** From the **Deployment Action** drop-down list, choose the action that you want to perform after defining the attributes for the circuit/VC. The options are:
- **Preview**—Displays the generated CLIs for each device. You can review the CLIs and decide if you want to edit any attributes or go ahead with the deployment.
  - **Deploy**—Deploys the configuration to the relevant devices immediately after you click **Submit** in the last page of the Provisioning Wizard.
- Step 13** Click **Next** to choose the endpoints and define the attributes based on the technology you have selected.
- Step 14** Click **Submit**. Depending on the deployment action you have chosen, the relevant action will be performed. That is, if you have chosen to preview the configuration, the preview page will be displayed where you can view the configurations, and then click **Deploy**. If you have chosen to deploy, the configurations will be directly deployed to the relevant devices.
- Step 15** (Optional) Click the **Leave this View** button to continue using Cisco EPN Manager and to enable the service deployment to continue in the background.
- Note** If the device is busy, the request from Cisco EPN Manager to deploy the service will wait up to a pre-configured period of time before the request times out. To change this setting, see [Set the Service Deployment Timeout Value](#), on page 433.

---

The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the  icon next to the circuit/VC name to see the Circuit/VC 360 view.

For information about how to create and provision circuit/VCs for various technologies, see:

- [Provision EVCs in a Carrier Ethernet Network](#), on page 436
- [Provision Circuits in an Optical/DWDM Network](#), on page 447
- [Provision L3VPN Services](#), on page 467
- [Provision Circuit Emulation Services](#), on page 483
- [Provision MPLS Traffic Engineering Services](#), on page 489

## Set the Service Deployment Timeout Value

When you deploy a service to devices, if the devices are pre-occupied or busy, the service request created waits for a pre-configured period of time to acquire a 'device lock' for deploying the service. By default, the timeout value is set to 60 minutes.

To change the default timeout value:

---

**Step 1** From the left sidebar, choose **Administration > Settings > System Settings**.

**Step 2** Expand the **Circuits/VCS** section and click **Deployment Settings**.

**Step 3** Set the required timeout value in minutes.

Cisco EPN Manager will now wait up to the specified time period to acquire the device lock for deploying the service. If the lock is not acquired within this time, the service deploy operation will fail.

---

## What Happens When a Deployment Fails

When you deploy a circuit/VC, Cisco EPN Manager performs configuration changes in the participating devices based on the type of circuit/VC. Only when the configuration changes are successfully deployed to the devices, the circuit/VC will be considered as successfully provisioned. If the deployment of configuration changes fails in any one of the participating device, Cisco EPN Manager rolls back the configuration changes made so far in all the devices.

Deployment action can result in any one of the following scenarios:

- Deployment succeeds in all the participating devices; roll back is not initiated—In this scenario, all devices are successfully configured and the circuit provisioning is successful.
- Deployment fails; roll back is initiated and succeeds—In this scenario, when configuring multiple devices, the configuration fails in one of the device. The failure could be due to various reasons, for example, the device has declined the configuration. Cisco EPN Manager identifies the failure and successfully rolls back all the configuration changes that were made on all the devices. In this scenario, all device configurations are restored to the states, which were there before the deployment was attempted.

Here is an example with three devices, A, B, and C, which are configured in a sequential order to provision a circuit. The configuration changes are deployed successfully in device A, but the deployment fails in device B. Cisco EPN Manager detects the failure and stops further configuration in devices B and C. It rolls back the configuration in the reverse order of provisioning, that is, it first rolls back the device B, followed by device A. Following are the actions that are performed sequentially in the three devices:

- Device C—Rollback is not required for device C because there were no changes deployed to the device. This is because the configuration failure was detected in device B before configurations changes were sent to device C.
- Device B—Cisco EPN Manager checks if there are any configuration changes made on this device before the deployment failed. If there are any changes, the partial configuration on this device is removed and the device is rolled back to the previous configuration.
- Device A—Cisco EPN Manager performs a complete roll back in device A, where all the configuration changes that were successfully deployed earlier are removed and the device is rolled back to the previous configuration.

- Deployment fails; roll back is initiated but fails— In this scenario, when the configuration deployment fails on any of the participating device(s), Cisco EPN Manager performs a roll back, but the roll back on one or more devices fail. Now, the device(s) on which the roll back had failed, has the partial configuration.

For example, the configuration changes are successfully deployed in devices A and B, the deployment fails in device C. Cisco EPN Manager identifies the failure and initiates the roll back in the reverse order of provisioning, that is, it first rolls back the device C, device B, and then device A. Following are the actions that are performed sequentially in the three devices:

- Device C—Cisco EPN Manager performs a successful roll back in device C.
- Device B—When attempting a rollback on device B, device connectivity is lost and there could be partial configurations left on the device.
- Device A—Cisco EPN Manager performs a rollback of Device A, even if the roll back fails in device B.

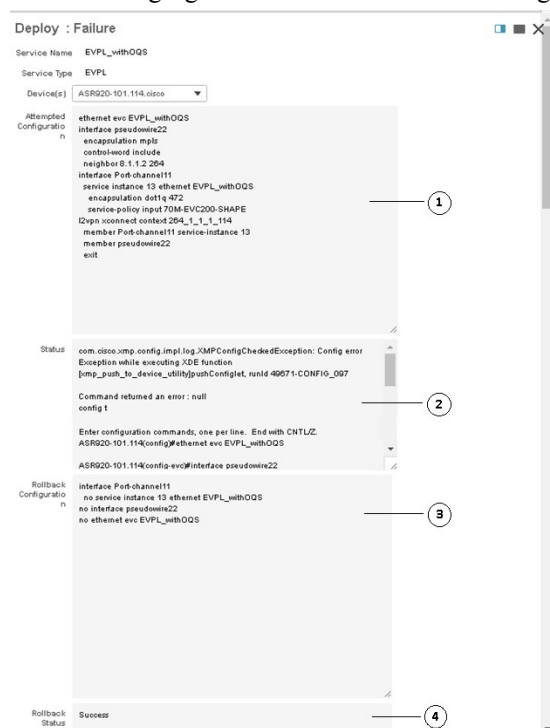


#### Note

The roll back may fail due to various other reasons.

In the Provisioning Wizard, after previewing the configurations, click **Deploy**. When the deployment fails, the rollback configuration and the status for each participating device is displayed. From the **Device(s)** drop-down list, choose the device for which you want to view the rollback configuration and the status.

The following figure illustrates the rollback configuration and the rollback status for each device.





1	Attempted Configuration— Shows the configurations that were deployed to the device selected in the <b>Device(s)</b> drop-down list.
2	Deployment Status— Shows the deployment status of the selected device. If the deployment succeeds, it shows the status as "Success". If the deployment fails, it provides information about the failure.
3	Roll back Configuration— Shows the configurations for which rollback is automatically attempted.
4	Roll back Status— Shows the roll back status of the selected device. If the roll back succeeds, it shows the status as "Success". If the roll back fails, it provides information about the failure. You can use this information to manually clean up the partial configurations on the device.

You can also click the *i* icon next to the **Provisioning** column in the Circuits/VCs and Deleted Circuits/VCs tabs in the extended tables to view the details of configuration, configuration errors, rollback configuration, and rollback configuration errors for each device participating in the circuit/VC. The *i* icon is available for all provisioning states, except None. For information about how to access the extended tables, see [View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map](#), on page 151.

For information about how to troubleshoot deployment and rollback failures, see [Troubleshoot Configuration Deployment Failures and Roll Back Failures](#), on page 435.

## Troubleshoot Configuration Deployment Failures and Roll Back Failures

Following are the tips to troubleshoot the deployment or roll back failures:

- Deployment fails, but roll back succeeds— If the configuration deployment fails, roll back is automatically initiated and the results are displayed in the results page. Analyse the attempted configuration and error message shown in the results page for each device and identify the root cause of the deployment failure.

The deployment failure could be due to, but not limited to the following issues:

- Invalid values entered for the service parameters in the Provisioning Wizard. For example, the Service ID may already exists or there could be semantic errors in the CLI that is generated, and so on.
- Device issues such as, device is not reachable, device password has changed, and so on.

In this case, you must locate the circuit (by the name that you had given when creating it) for which deployment has failed, edit the circuit, and re-attempt the provisioning. If the service parameter for which the value to be changed is not editable, delete the circuit and create a new circuit.




---

**Note** Before deleting the circuit, ensure that it is not in use.

---

- Both, deployment and roll back fails— In this case, do the following:
  1. Ensure that the device is reachable and perform a device re-synch.
  2. If there were any device issues that were reported in the previous deployment, try to fix the issues.
  3. Edit the circuit and update the attributes, if required, and then re-attempt the circuit deployment.
  4. If the deployment fails, Cisco EPN Manager will initiate the roll back.

5. If the roll back fails again, identify the cause of the roll back failure.
6. To identify the cause of the failure, you can use the configuration and roll back transaction details, history of the service deployment attempts, and the roll back attempts that are displayed in the Circuit/VC 360 view. See [Get Quick Information About a Circuit/VC: Circuit/VC 360 View](#), on page 528.
7. Manually remove the partial configurations that are stored on the device.

You can also contact the Cisco representative to analyse and identify the root cause of configuration deployment failure and roll back failure.

## Provision EVCs in a Carrier Ethernet Network

- [Summary of Cisco EPN Manager Carrier Ethernet Provisioning Support](#) , on page 436
- [Prerequisites for EVC Provisioning](#), on page 436
- [Create and Provision a New Carrier Ethernet EVC](#), on page 437
- [Create and Provision an EVC with Multiple UNIs](#), on page 439

## Summary of Cisco EPN Manager Carrier Ethernet Provisioning Support

This topic provides a summary of the Carrier Ethernet service provisioning support in Cisco EPN Manager 2.1. For a more detailed overview of the different types of EVCs and the supported underlying networks, see [Overview of Circuit/VC Discovery and Provisioning](#), on page 415.

Cisco EPN Manager supports provisioning of both port-based and VLAN-based VCs of the following types:

- E-line—Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL). See [E-Line](#), on page 417.
- E-LAN—EP-LAN and EVP-LAN. See [E-LAN](#), on page 417.
- E-Access—Access EPL and Access EVPL. See [E-Access](#), on page 418.
- E-TREE—EP-TREE and EVP-TREE. See [E-Tree](#), on page 418.

Cisco EPN Manager supports the following supplementary provisioning functions that can be used during EVC creation:

- Provision UNIs—For each EVC, you must define the attributes of the participating UNIs. You can either do this during the EVC creation or you can provision a UNI independently of the EVC creation process. See [Configure a Device and Interface To Be a UNI](#), on page 445.
- Provision ENNI—For E-Access circuits, you must define the attributes of the ENNI. You can either do this during the EVC creation or you can provision an ENNI independently of the EVC creation process. See [Configure a Device and Interface To Be an ENNI](#), on page 446.
- QoS Profiles—You can create QoS profiles to apply to VCs. See [Create QoS Profiles](#), on page 510.
- EVC Attribute Profiles—You can create profiles containing all the required attributes for an EVC. These profiles can be selected during EVC creation to define the attributes of the EVC, instead of having to define the attributes individually for each EVC. See [Create Circuit/VC Profiles](#) , on page 509.

## Prerequisites for EVC Provisioning

The following prerequisites must be met before you can provision EVCs:

1. Communication between devices must be set up before you can provision EVCs:
  - In an MPLS end-to-end network, Label Distribution Protocol (LDP) must be set up across the network and each device must be provided with an LDP ID. This enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding. Alternatively MPLS end-to-end connectivity can be achieved using MPLS Traffic Engineering or segment routing, and specifically, EVC provisioning over unidirectional or bidirectional TE tunnels is supported.
  - If there is Ethernet access, i.e., not all devices are MPLS-enabled, G.8032 rings or ICCP-SM must be configured to connect the Ethernet access switch to the MPLS switch.
  - CDP or LLDP must be configured on the links within the G.8032 ring to enable Ethernet link discovery.
2. To provision EVCs over ICCP-SM and G.8032 networks, all VLANs (from 1 to 4095) should be configured either as primary or as secondary VLANs.
3. Inventory collection status for the devices on which the EVCs will be provisioned must be *Completed*. To check this, go to **Inventory > Network Devices**, and look at the status in the Last Inventory Collection Status column.
4. Customers can be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. Choose **Inventory > Other > Customers** in the left sidebar to create and manage customers.
5. For interfaces to be used in EVCs, it is recommended to reset the default configuration on the interfaces. In global configuration mode, configure the following command on each interface:

```
default interface 'interface-name'
```

6. For ME3600 and ME3800 devices, service instances can only be configured on trunk ports with no allowed VLANs. Configure the following commands on the interface and then re-sync the device in Cisco EPN Manager :

```
interface GigabitEthernetXX/XX
switchport trunk allowed vlan none
switchport mode trunk
```

## Create and Provision a New Carrier Ethernet EVC

EVCs are created in the context of the topology map. You can access the topology map and the Provisioning Wizard by choosing **Configuration > Network > Service Provisioning** in the left sidebar or you can open the Provisioning Wizard from the topology map, as described in the procedure below.

The process of creating and provisioning an EVC is similar for all supported EVC types and involves:

- Specifying the endpoints (UNIs and ENNIs) of the EVC.
- Defining the configuration parameters of the circuit/VC.

### Before you begin

For information about the prerequisites that must be met before you can provision EVCs, see [Prerequisites for EVC Provisioning, on page 436](#).

To create a new EVC:

- Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click the Device Groups button in the toolbar and select the group of devices you want to show on the map.
- Step 3** In the Circuits/VCs tab, click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.
- Step 4** Select **Carrier Ethernet** in the Technology drop-down list. Cisco EPN Manager displays a list of relevant circuit/VC types in the Service Type area. For example, Carrier Ethernet service types include EPL, EVPL, EP-LAN, and so on.
- Step 5** In the Service Type list, select the type of circuit/VC you want to create.
- Step 6** If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See [Create Circuit/VC Profiles](#), on page 509.
- Step 7** Click **Next** to go to the Service Details page.
- Step 8** (Optional) Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.
- Step 9** Enter the Service Details. See [Service Details Reference](#), on page 441 for descriptions of the fields and attributes.
- Step 10** For E-Line, E-Tree, and E-LAN EVCs: If required, configure the service OAM which enables fault and performance monitoring across the EVC. For E-Line EVCs, select the Enable CFM check box to enable the Service OAM options. You can then choose to either create a new CFM domain or select an existing domain for the E-Line EVC. See [Service OAM](#), on page 444. Click the Plus icon to add a row to the Service OAM table and provide values in the relevant columns. For E-Tree EVCs, you must specify the direction, i.e., Leaf-to-Root, Root-to-Leaf, or Root-to-Root.
- Step 11** In the Deployment Action field, specify what you want to do when the EVC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.
- Step 12** Click **Next** to go to the page(s) in which you define the UNI(s). In the case of E-Access, there is an additional page for defining the ENNI.
- Step 13** Identify the device and interface that will serve as the UNI:
- Note** If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, select the Unmanaged check box and provide information for the unmanaged device. See [Provision a Circuit/VC with an Unmanaged Endpoint](#), on page 511
- If you have already configured the required interface on the device as a UNI, uncheck the **Create New UNI** check box and select the relevant UNI Name from the list.
  - To create a new UNI:
    - Make sure that the **Create New UNI** check box is checked.
    - In the UNI Name field, enter a name for the UNI that will enable easy identification of the UNI.
    - Select a device from the list in the Device field or click on a device in the map to select it and populate the Device field. A list of the selected device's ports is displayed.
    - Select the required port from the Port table. If the port cannot be used for the UNI, there is an alert icon next to the UNI name in the Port table that displays the reason why the port cannot be selected.
- Note** The device you select during UNI creation is circled in orange in the map. The UNI name is displayed above the orange circle. If it is a point-to-point EVC, the orange circle is labeled to indicate whether it is an A-side or Z-side endpoint.
- Step 14** If you are creating a new UNI, enter the New UNI Details. See [New UNI Details Reference](#), on page 442 for descriptions of the fields and attributes.
- Step 15** Enter the UNI Service Details. See [UNI Service Details Reference](#), on page 443 for descriptions of the fields and attributes.

- Step 16** If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager , select the **Unmanaged** check box and provide information for the unmanaged device. See [Provision a Circuit/VC with an Unmanaged Endpoint, on page 511](#) for more information.
- Step 17** For E-LAN and E-TREE EVCs with H-VPLS as the core technology, select the devices that will serve as the primary and secondary hubs.
- Step 18** For E-Line and E-Access EVCs: In the Pseudowire Settings page, you can select a TE tunnel over which the EVC will traverse, as follows:
1. Check the **Static Preferred Path** check box to assign a static route for the service.
  2. Choose the Preferred Path Type as Bidirectional or Unidirectional.
  3. Select the required bidirectional TE tunnel from the Preferred Path drop-down list. This list contains all existing bidirectional TE tunnels between the endpoints of the EVC.  
**Note** This field is available only if you selected **Bidirectional** as the Preferred Path Type.
  4. Select the required unidirectional TE tunnels from the Preferred Path (A-Z) and Preferred Path (Z-A) drop-down lists.  
**Note** These fields are available only if you selected **Unidirectional** as the Preferred Path Type.
  5. Select the **Allow Fallback to LDP** check box if you want the default path to be used if the preferred path is unavailable.  
**Note** If no tunnel exists between the endpoints, the Preferred Path and the Fallback to LDP options will be disabled.
  6. Select the **Send Control Word** check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.
  7. Select the **Interworking Option** if you need to interconnect sites using either Ethernet, VLAN, or IP. This option must be enabled if one of the endpoints in the EVC is an unmanaged device.
  8. Enter the required bandwidth for the pseudowire.
- Step 19** (Optional) If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the Service Template page. See [Extend a Circuit/VC Using Templates, on page 512](#) for more information.
- Step 20** When you have provided all the required information for the circuit/VC, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.
- Step 21** The circuit/VC should be added to the list in the Circuits/VCs tab in the Network Topology window.

---

If the configuration deployment fails, see the [What Happens When a Deployment Fails, on page 433](#) section.

## Create and Provision an EVC with Multiple UNIs

Cisco EPN Manager supports creating/selecting multiple UNIs during the creation and provisioning of multipoint EVCs (E-LAN and E-Tree).



**Note** You can have multiple UNIs on the same device for EVCs using VPLS as the core technology, but not for H-VPLS-based EVCs.

### Before you begin

For information about the prerequisites that must be met before you can provision EVCs, see [Prerequisites for EVC Provisioning, on page 436](#).

To create a new EVC:

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.  
The network topology window opens.
- Step 2** From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.
- Step 3** Click the **Circuits/VCs** tab.
- Step 4** From the **Circuits/VCs** pane toolbar, click the + (**Create**) icon.  
The Provisioning Wizard opens in a new pane to the right of the map.
- Step 5** Select **Carrier Ethernet** in the Technology drop-down list
- Step 6** In the Service Type list, select a multipoint EVC type.
- Step 7** If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See [Create Circuit/VC Profiles, on page 509](#).
- Step 8** Click **Next** to go to the Service Details page.
- Step 9** Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.
- Step 10** Enter the Service Details. See [Service Details Reference, on page 441](#) for descriptions of the fields and attributes.
- Step 11** In the Deployment Action field, specify what you want to do when the EVC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.
- Step 12** Click **Next** to go to the page(s) in which you define the UNI(s).
- Step 13** In the Multi UNI area, click the Plus icon to add the first UNI to the table. The UNI is given a default name and is automatically selected in the table. Each time you click the Plus icon, a new UNI is added to the table.  
  
Alternatively, you can click on devices in the map to add new UNIs to the table. In this case, the device name will be populated in the Device field under New UNI details.
- Step 14** Select a UNI in the table to define or edit its attributes.
- Step 15** Identify the device and interface that will serve as the UNI:
- To use an existing UNI, uncheck the Create New UNI check box and select the relevant UNI Name from the list.
  - To define a new UNI:
    - Make sure that the Create New UNI check box is checked.
    - In the UNI Name field, enter a name for the UNI that will enable easy identification of the UNI.
    - Select a device from the list in the Device field. A list of the selected device's ports is displayed.

- Select the required port from the Port table. If the port cannot be used for the UNI, there is an alert icon next to the UNI name in the Port table that displays the reason why the port cannot be selected.

- Step 16** If you are creating a new UNI, enter the New UNI Details. The New UNI details are relevant for the UNI that is currently selected in the Multi UNI table. See [New UNI Details Reference, on page 442](#) for descriptions of the fields and attributes.
- Step 17** Enter the UNI Service Details. See [UNI Service Details Reference, on page 443](#) for descriptions of the fields and attributes. Click Next.
- Step 18** If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager , provide information for the unmanaged device in the Unmanaged page. See [Provision a Circuit/VC with an Unmanaged Endpoint, on page 511](#)
- Step 19** Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the Service Template page. See [Extend a Circuit/VC Using Templates](#) for more information.
- Step 20** When you have provided all the required information for the circuit/VC, click Submit. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.
- Step 21** The circuit/VC should be added to the list in the Circuits/VCS pane in the Network Topology window.

## Service Details Reference

The following table lists and describes the attributes that define the EVC on the service level. Note that not all attributes are relevant for all the EVC types.

**Table 28: Service Details**

Attribute	Description
Service Name	Unique name to identify the circuit/VC.
Service Description	Description of the VC that will help to identify the VC.
Service Type	Prepopulated based on the type of service you are creating—EPL, EVPL, EP-LAN, and so on.
Service MTU	The maximum size, in bytes, of any frame passing through the VC. Values can be between 1522 and 9216. The service MTU must be lower than or equal to the MTU defined on all of the service's UNIs.
Core Technology	VPLS or H-VPLS. See <a href="#">Core Technology for Multipoint EVCs, on page 416</a> .
VPN ID	Relevant for multipoint EVCs (both VPLS and H-VPLS). This field is automatically populated with the next available pseudowire ID. This ID can be changed during the EVC creation process (valid value range: 1-4294967295). The ID is not editable when modifying the EVC.  <b>Note</b> The VPN ID is used uniquely across the network, meaning that two services will not use the same VPN ID. In addition, the VPN ID cannot use a pseudowire ID which is already configured in the network to avoid pseudowire ID collision.
Bundling	Enables multiple VLANs on this VC. Multiple CE-VLAN IDs are bundled to one EVC.



Attribute	Description
CE-VLAN ID Preservation	Ensures that the CE-VLAN ID of an egress service frame is identical in value to the CE-VLAN ID of the corresponding ingress service frame. This must be enabled if bundling is enabled.
CE-VLAN ID CoS Preservation	Ensures that the CE-VLAN CoS of an egress service frame is identical in value to the CE-VLAN CoS of the corresponding ingress service frame. The CoS markings are unaltered.

## New UNI Details Reference

The following table lists and describes the attributes relating to the port that is specified as the UNI. Note that not all attributes are relevant for all the EVC types.

**Table 29: New UNI Details**

Attribute	Description
MTU	The Maximum Transmission Size, in bytes, of a packet passing through the interface. The MTU of the UNI must be greater than or equal to the MTU defined on the service level.
Auto Negotiation	Check this check box to automatically negotiate the speed and duplex mode.
Speed	Port speed. You can reduce the speed if this is supported on the port. <b>Note</b> This field is not available if you select the Auto Negotiation check box.
Duplex Mode	<ul style="list-style-type: none"> <li>Full Duplex—Uses simultaneous communication in both directions between the UNI and the customer's access switch, assuming that both sides support full duplex. If one side does not support full duplex, the port will be brought down.</li> <li>Auto-Negotiation—Uses the mode that is agreed upon between the two devices, depending on what is supported. Full Duplex will be attempted but if one device does not support it, half duplex will be used.</li> </ul> <b>Note</b> This field is not available if you select the Auto Negotiation check box.
Service Multiplexing	Allows the UNI to participate in more than one EVC instance.
UNI Allows Bundling	Allows the UNI to participate in VCs with Bundling enabled. See Bundling in <a href="#">Service Details Reference, on page 441</a>
Untagged CE-VLAN ID	The ID of the CE-VLAN assigned to untagged traffic.
Ingress/Egress QoS Profile	Select the required QoS profile for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. Refer to <a href="#">Create QoS Profiles, on page 510</a> for information on how to create QoS profiles.
UNI QoS Profile	Applies a QoS profile on the UNI itself to define the bandwidth profile and other quality of service attributes of the UNI. If you apply a QoS profile on the UNI level, you should not apply a QoS profile on the service level.
Enable Link OAM	Enables IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this UNI and the customer's access switch.



Attribute	Description
Enable Link Management	Enables the customer access switch to get information about this UNI, VLAN IDs, services on the UNI, and so on.

## UNI Service Details Reference

The following table lists and describes the attributes of the EVC in relation to the UNI, i.e., how the EVC operates on this UNI. Note that not all attributes are relevant for all the EVC types.



**Note** For QinQ attributes, only the attributes that are supported on the selected device will appear in the wizard.

**Table 30: UNI Service Details**

Attribute	Description	Additional Information
Ingress/Egress Service QoS Profile	Select the required QoS profile for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. Refer to <a href="#">Create QoS Profiles, on page 510</a> for information on how to create QoS profiles.	
Layer 2 Control Protocol Profile	Profile that determines how the various communication protocols are handled. Frames using the various protocols are either tunneled, dropped or peered. Refer to MEF 6.1 for details.	
Designation	For E-Tree: Select the role of the UNI in the VC, either Leaf or Root.	
Use point to point connection with Root	For E-Tree: If the UNI is designated as a leaf, you can select this check box to create an active pseudowire between root and leaf. The check box will not appear if there is more than one endpoint on a single device or if there is more than one root in the service.	
Match	Select the type of tagging the traffic should have in order to enter the UNI: <ul style="list-style-type: none"> <li>• Dot1q—Mapping of 802.1q frames ingress on an interface to the service instance.</li> <li>• Dot1ad—Mapping of 802.1ad frames ingress on an interface to the service instance.</li> <li>• Default—Traffic that is not assigned to any other VC on this port.</li> <li>• Untagged—Frames that have no VLAN tag</li> </ul>	Dot1AD is not supported on ME3600 devices running 15.3(3) software version.
Auto Allocate VLAN	Check this check box to automatically allocate a VLAN ID for the UNI.	
VLAN(s)	VLAN identifier, an integer between 1 and 4094. You can enter a range of VLAN IDs using a hyphen or a comma-separated series of VLAN IDs.	This field is not available if you have checked the Auto Allocate VLAN check box.

Attribute	Description	Additional Information
Inner VLAN(s)	VLAN identifier for the second level of VLAN tagging, an integer between 1 and 4094. You can enter a range of VLAN IDs using a hyphen or a comma-separated series of VLAN IDs.	
Untagged Bundled	Enables traffic with no VLAN tags to be bundled together with VLAN tagged frames.	
Priority Tagged Bundled	Enables priority tagged traffic to be bundled together with VLAN tagged frames.	
Exact	Prevents admittance of traffic with additional inner VLAN tags other than those that are matched to be carried by the service.	Applicable for IOS-XR devices only.
Outer VLAN CoS	The outer VLAN Class of Service identifier that should be associated with the frame. The CoS ID can be an integer between 0 and 7.	Applicable for IOS devices only.
Inner VLAN CoS	The inner VLAN Class of Service identifier that should be associated with the frame. The CoS ID can be an integer between 0 and 7.	Applicable for IOS devices only.
E-Type	Limits the service to only carry frames of the specified Ethertype: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> <li>• PPPoE-All</li> <li>• PPPoE-Discovery</li> <li>• PPPoE-Session</li> </ul>	Applicable for IOS devices only.
Rewrite Definition Action	The encapsulation adjustment to be performed when the frame enters the UNI: <ul style="list-style-type: none"> <li>• None</li> <li>• Pop—Removes one or two VLAN tags from the frame on ingress and adds them on egress.</li> <li>• Push—Adds one or two VLAN tags from the frame on ingress and removes them on egress., either Dot1q or Dot1ad tags.</li> <li>• Translate—Replaces VLAN tags with new VLAN tags, either Dot1q or Dot1ad tags. The translation can be 1:1, 1:2, 2:1, or 2:2.</li> </ul>	The Translate action is applicable for IOS-XR devices only.

## Service OAM

On the service level, you can define EOAM (Ethernet Operations, Administration and Management) parameters that will allow monitoring and troubleshooting of the EVC. Effectively, you will be configuring Connectivity Fault Management (CFM) components on the endpoints of the EVC.

For a point-to-point EVC, you can define OAM parameters in one direction, i.e., from UNI A to UNI Z or in both directions. For a multipoint EVC, you can define the source and destination MEP groups and then associate the EVC endpoints with a specific MEP group.

See [Configure EOAM Fault and Performance Monitoring, on page 362](#) for more information about CFM and for device-level CFM configuration.

Use the Service OAM section in the Customer Service Details page of the Provisioning Wizard to define the specifications of the service frame to be monitored and to define the OAM profile to apply to that frame, as follows:

- From—The source of the traffic flow across the EVC.
- To—The destination of the traffic flow across the EVC.
- Direction (E-Tree only) —The direction of traffic flow between leaf and root, or root to root.

**Note**

Your input in the From and To fields creates MEP groups, or ordered sets of UNIs. In the next page of the wizard, you will associate the UNI with one of these MEP groups.

- CoS—The Class of Service identifier that should be associated with the frame.
- OAM Profile—A set of OAM attributes that should be applied to the frame to enable performance monitoring. The following OAM profiles are available for selection:
  - Performance Monitoring 1: Enables continuity check and synthetic loss measurement.
  - Performance Monitoring 2: Enables continuity check, synthetic loss measurement, and single-ended delay measurement.
  - Performance Monitoring 3: Enables continuity check, synthetic loss measurement, and dual-ended delay measurement.
- Continuity Check Interval—The interval between continuity check messages.

## Configure a Device and Interface To Be a UNI

The User Network Interface (UNI) is the physical demarcation point between the responsibility of the Subscriber (the Customer Edge or CE) and the responsibility of the Service Provider (the Provider Edge or PE).

UNIs demarcate the endpoints of EVCs, so configuring device interfaces as UNIs is an essential part of VC provisioning. UNI configuration can be done during the VC creation process. Alternatively, you can configure UNIs independently of VC creation. These UNIs will be available for selection during VC creation.

To configure a UNI:

- 
- Step 1** Follow the instructions in [Create and Provision a New Carrier Ethernet EVC, on page 437](#) to access the Provisioning Wizard.
  - Step 2** Select **Carrier Ethernet** from the Technology drop-down list.
  - Step 3** Select **UNI** from the Service Types list.
  - Step 4** Click **Next** to go to the Customer Service Details page.
  - Step 5** Provide a unique name and description for the UNI, and associate it with a customer, if required.
  - Step 6** Define the service attributes of the UNI, as follows:
    - All to One Bundling—For port-based VCs where the UNI is dedicated to the VC. When enabled, all CE-VLAN IDs are bundled to one VC. When All to One Bundling is selected, Multiplexing and Bundling cannot be selected.
    - Service Multiplexing—For VLAN-based VCs where the UNI is shared between multiple VCs. When enabled, allows the UNI to participate in more than one EVC instance.
    - Bundling—Allows the use of multiple VLANs for this UNI. Multiple CE-VLAN IDs are bundled to one EVC.

- Step 7** Under Deploy, select whether you want to deploy the UNI immediately upon completion or first display a preview of the CLI that will be deployed to the device.
- Step 8** Click **Next** to go to the UNI Details definition page.
- Step 9** Select the device and port you want to configure as the UNI.
- Step 10** Configure the UNI attributes, as described in [New UNI Details Reference, on page 442](#).
- Step 11** Click **Submit**. If you previously chose to deploy the circuit upon completion, a job is created and the required CLI is deployed to the devices. If you chose to see a preview of the CLI before actually deploying to the devices, the preview will be displayed now. Verify the CLI and if you want to change any of the attributes, click **Edit Attributes**. Else, click **Deploy**.

## Configure a Device and Interface To Be an ENNI

The External Network to Network Interface (ENNI) specifies the reference point that is the interface between two Metro Ethernet Networks (MENs) where each operator network is under the control of a distinct administration authority. The ENNI is intended to support the extension of Ethernet services across multiple operator MENs, while preserving the characteristics of the service.

When provisioning an E-Access VC, you need to define the ENNI that will carry traffic through to the adjacent network. ENNI configuration can be done during the VC creation process. Alternatively, you can configure ENNIs independently of VC creation. These ENNIs will be available for selection during VC creation.

To configure an ENNI:

- Step 1** Follow the instructions in [Create and Provision a New Carrier Ethernet EVC, on page 437](#) to access the Provisioning Wizard.
- Step 2** Select **Carrier Ethernet** from the Technology drop-down list.
- Step 3** Select **ENNI** from the Service Types list.
- Step 4** Click **Next** to go to the Customer Service Details page.
- Step 5** Provide a unique name and description for the ENNI, and associate it with a customer/operator, if required.
- Step 6** Under Deploy, select whether you want to deploy the ENNI immediately upon completion or first display a preview of the CLI that will be deployed to the device.
- Step 7** Click **Next** to go to the ENNI Details definition page.
- Step 8** Select the device and port(s) you want to configure as the ENNI.
- Step 9** Define the following parameters for the ENNI:
- **MTU**—The Maximum Transmission Size, in bytes, of a packet passing through the interface. The MTU of the ENNI must be greater than 1526.
  - **Speed**—If required, you can reduce the speed of the port if this is supported.
  - **Protection Mechanism**—This defines the resiliency scheme at the ENNI. If you have selected more than one port for this ENNI, you can specify whether to apply a protection mechanism, which could be Link Aggregation or another agreed upon protection mechanism. Selecting Link Aggregation creates a Link Aggregation Group (LAG) with two links. If one of the links fails, traffic is moved to the other link.
- Step 10** Click **Submit**. If you previously chose to deploy the circuit upon completion, a job is created and the required CLI is deployed to the devices. If you chose to see a preview of the CLI before actually deploying to the devices, the preview

will be displayed now. Verify the CLI and if you want to change any of the attributes, click **Edit Attributes**. Else, click **Deploy**.

## Provision Circuits in an Optical/DWDM Network

- [Summary of Cisco EPN Manager Optical/DWDM Network Provisioning Support, on page 447](#)
- [Prerequisites for Provisioning Optical Circuits, on page 448](#)
- [Create and Provision an OCH Circuit, on page 449](#)
- [Create and Provision Two Mutually Diverse OCH-Trail UNI Circuits, on page 454](#)
- [Create and Provision a Media Channel Group SSON Circuit, on page 456](#)
- [Create and Provision a Media Channel SSON Circuit, on page 457](#)
- [Create and Provision an OTN Circuit, on page 460](#)
- [Create and Provision an ODU Circuit, on page 466](#)

## Summary of Cisco EPN Manager Optical/DWDM Network Provisioning Support

Cisco EPN Manager supports the provisioning of Dense Wavelength Division Multiplexing (DWDM) optical channel (OCH) circuit types. The DWDM optical technology is used to increase bandwidth over existing fiber optic backbones. It combines and transmits multiple signals simultaneously at different wavelengths on the same fiber. In effect, one fiber is transformed into multiple virtual fibers.

Cisco EPN Manager supports the following optical circuits:

- Dense Wavelength Division Multiplexing (DWDM) optical channel (OCH) circuit—Following are the different optical channel circuit types:
  - Optical Channel Network Connection (OCHNC) WSON—OCHNC WSON circuits establish connectivity between two optical nodes on a specified C-band wavelength. For more information, see [Optical Channel Network Connection \(OCHNC\) WSON, on page 420](#).
  - Optical Channel Client Connection (OCHCC) WSON—OCHCC WSON circuits extend the OCHNC WSON to create an optical connection from the source client port to the destination client port of the TXP/MXP cards. For more information, see [Optical Channel Client Connection \(OCHCC\) WSON, on page 420](#).
  - Optical Channel (OCH) Trail WSON—OCH trail WSON circuits transport the OCHCC WSON circuits. For more information, see [Optical Channel \(OCH\) Trail WSON, on page 421](#).
  - Optical Channel (OCH) Trail connecting NCS 1002, NCS 55xx, and ASR 9K devices—This OCH trail circuit creates an optical connection from the source trunk port of an NCS 1002, NCS 55xx, or ASR 9K device to the destination trunk port of another similar device. For more information, see [Optical Channel \(OCH\) Trail Connecting NCS 1002, NCS 55xx, and ASR 9K Devices, on page 421](#).
  - Optical Channel (OCH) Trail User-to-Network Interface (UNI)—An OCH trail UNI circuit establishes connectivity between Cisco NCS 2000 series devices and Cisco NCS 4000 series devices. For more information, see [Optical Channel \(OCH\) Trail User-to-Network Interface \(UNI\), on page 422](#).
  - Spectrum Switched Optical Network (SSON)—SSON circuits allow you to provide more channels in a span. Using the SSON functionality, the circuits are placed closer to each other if they are created within a media channel group. For more information, see [Spectrum Switched Optical Network \(SSON\) Circuits, on page 422](#).

- **Optical Transport Network (OTN)**—An OTN circuit can be established statically or dynamically between ingress and egress nodes using Resource Reservation Protocol (RSVP) signaling. For more information, see [Optical Transport Network \(OTN\) Circuit, on page 423](#).
- **Optical Channel Data Unit User-to-Network Interface (ODU UNI)**—An ODU UNI circuit represents the actual end-to-end client service passing through the OTN architecture. For more information, see [Optical Channel Data Unit User-to-Network Interface \(ODU UNI\), on page 424](#).
- **Optical Channel Data Unit (ODU) Tunnel**—ODU tunnel circuits transport the ODU UNIs. For more information, see [Optical Channel Data Unit \(ODU\) Tunnel, on page 424](#).
- **Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU)**—OPU over ODU circuits provide a high-bandwidth point-to-point connection between two customer designated premises. These circuits use ODU UNI circuits to carry client signals through the network. For more information, see [Optical Channel Payload Unit \(OPU\) Over Optical Channel Data Unit \(ODU\), on page 425](#).
- **Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin**—An ODU UNI Hairpin circuit is similar to an ODU UNI circuit, but it is created in the management plane and it is an intra node circuit, that is, the source and destination is the same device but with different interfaces. For more information, see [Optical Channel Data Unit User-to-Network Interface \(ODU UNI\) Hairpin, on page 425](#).
- **Optical Channel Data Unit (ODU)**—Optical Channel Data Unit (ODU) is created as a sub controller of an OTU controller. ODU contains information for the maintenance and operational functions to support optical channels. For more information, see [Optical Channel Data Unit \(ODU\), on page 425](#).

## Prerequisites for Provisioning Optical Circuits

Following are the prerequisites for provisioning an optical circuit:

- Cisco EPN Manager supports both, Wavelength Switched Optical Network (WSON) and non-WSON circuits. However, for non-WSON circuits, Cisco EPN Manager supports only circuit discovery, which includes circuit overlay, circuit 360 view, multilayer trace view, and circuit details. Cisco EPN Manager does not support the provisioning, activation, deactivation, protection switch actions, and modification of non-WSON circuits.
- Communication between devices must be set up before you can provision an optical circuit.
- Inventory collection status for the devices on which the optical circuits will be provisioned must be Completed. To check this, go to **Inventory > Device Management > Network Devices**, and look at the status in the Last Inventory Collection Status column.
- DWDM grid unit must be set to either, wavelength or frequency. To do this, go to **Administration > Settings > System Settings > Circuits/VCS Display**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Terahertz (THz))**.
- Before you provision an OCHNC or a Media Channel NC circuit using NCS 2000 series devices running on software version 10.7 or later, ensure that you create a UNI config, either in Cisco Transport Controller (CTC) or in Cisco EPN Manager.
- Optionally, customers must be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. From the left sidebar, choose **Inventory > Other > Customers** to create and manage customers.

# Create and Provision an OCH Circuit

To provision an OCH circuit:

## Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see [Prerequisites for Provisioning Optical Circuits, on page 448](#).

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click **Device Groups**, and then select the location in which you want to create the OCH circuit.
- Step 3** Close the **Device Groups** popup window.
- Step 4** In the **Network Topology** window, click **Circuits/VCs**.
- Step 5** Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.
- You can also access the Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.
- Step 6** From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, Optical service types for OCH circuits include OCHNC WSON, OCHCC WSON, OCH-Trail WSON, and OCH-Trail UNI.
- Step 7** In the **Service Type** area, choose the type of OCH circuit you want to create.
- Step 8** If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles , on page 509](#).
- Step 9** Click **Next** to go to the **Customer Section** page.
- Step 10** (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.
- Step 11** Enter the circuit name and its description in the **Customer Section** page.
- Step 12** Click **Next** to go to the **Circuit Section** page.
- Note** If you select OCH-Trail UNI as the optical service type, the **Endpoint Section** page appears first followed by the **Circuit Section** page.
- Step 13** Enter the circuit details. See [Circuit Section Reference for OCH Circuit Types, on page 450](#) for descriptions of the fields and attributes.
- Step 14** Click **Next** to go to the **Endpoint Section** page.
- Step 15** Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name, Termination Point, Add/Drop Port, OCH-Trail, and Side columns. The Side column gets auto-populated based on the port selected. Only network elements that are available and compatible with the circuit type you chose will be displayed.
- Note** The **Add Port** and **Drop Port** columns are available only for OCHNC WSON circuit. Once you choose the port that needs to be added to the Add Port column, the values in the Drop Port and Side columns get auto-populated. Also, you can manually edit the values in the Drop Port column.
- Step 16** Select a trail diversity for the OCH circuit. The OCH circuit that you are creating will be diverse from the trail that you choose.
- Note** You cannot modify or delete the trail diversity once it is created.

**Step 17** Click **Next** to go to the **Constraints Section** page.

**Step 18** Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

**Note** When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

**Step 19** Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it but you cannot edit the attributes.

**Step 20** The circuit should be added to the list in the Circuits/VCS pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

## Circuit Section Reference for OCH Circuit Types

The following table lists and describes the attributes that define the OCH circuit types.

**Table 31: Circuit Section Reference—OCH Circuit Types**

Attribute	Description	Enabled
<b>Circuit Details</b>		
Label	Unique name to identify the circuit.	
State	Administrative state for the circuit. Values are: <ul style="list-style-type: none"> <li>In Service—The circuit is in service and able to carry traffic.</li> <li>Out of Service—The circuit is out of service and unable to carry traffic.</li> </ul>	For all OCH circuit types.
Bi-directional	Check this check box to create a two-way circuit.	For OCHCC WSON and OCH Trail WSON circuit types.



Attribute	Description	Enabled
Protection	<p>Protection mechanism for the circuit. Cisco EPN Manager supports the following protection mechanism based on the circuit type selected:</p> <ul style="list-style-type: none"> <li>• None—For unprotected circuits. This value is available for all OCH circuit types..</li> <li>• PSM—When a Protection Switch Module (PSM) card is connected to a TXP card. This value is available for OCHNC WSON and OCHCC WSON circuit types.</li> <li>• Y-Cable—When a transponder or muxponder card protects the circuit. This value is available for OCHCC WSON circuit type.</li> <li>• Splitter—When a MXPP/TXPP card is used. The circuit source and destination are on MXPP_MR_2.5G and TXPP_MR_2.5G cards. These cards provides splitter (line-level) protection (trunk protection typically on TXPP or MXPP transponder cards). This value is available only for OCHCC WSON circuit type.</li> </ul>	For OCHNC WSON circuit type.
<b>Route Properties</b>		
Diverse From Tunnel	Select a tunnel to ensure that it is not used by the circuit you are provisioning. This is to ensure that if there is a failure in a tunnel, the same tunnel is not used by another circuit.	For OCH-Trail UNI circuit types when the Mutual Diversity check box is unchecked.
Validation	<p>Validation mode for the circuit. Values are:</p> <ul style="list-style-type: none"> <li>• Full—The circuit is created when the circuit validation result is greater than or equal to the acceptance threshold value.</li> <li>• None—The circuit is created without considering the acceptance threshold value.</li> </ul>	For all OCH circuit types.
Acceptance Threshold	<p>Protection acceptance threshold value set for the OCH protected circuits. Values are:</p> <ul style="list-style-type: none"> <li>• Green—Indicates that the restoration failure risk is 0%.</li> <li>• Yellow—Indicates that the restoration failure risk is between 0% and 16%.</li> <li>• Orange—Indicates that the restoration failure risk is between 16% and 50%.</li> <li>• Red—Indicates that the restoration failure risk is greater than 50%.</li> </ul>	For all OCH circuit types when the Validation field is set to Full.

Attribute	Description	Enabled
Protect Acceptance Threshold	Protection acceptance threshold value set for the OCH protected circuits. Values are: <ul style="list-style-type: none"> <li>• Green—Indicates that the restoration failure risk is 0%.</li> <li>• Yellow—Indicates that the restoration failure risk is between 0% and 16%.</li> <li>• Orange—Indicates that the restoration failure risk is between 16% and 50%.</li> <li>• Red—Indicates that the restoration failure risk is greater than 50%.</li> </ul>	For OCHNC WSON circuit type when: <ul style="list-style-type: none"> <li>• Protection field is set to PSM, Y-Cable, or Splitter..</li> <li>• Validation field is set to Full.</li> </ul>
Ignore Path Alarms	Check the check box to ignore path alarms.	For OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types.
Allow Regeneration	Check the check box to allow the network elements to regenerate the signal.	For all OCH circuit types.
Restoration	Check this check box to restore the failed OCH circuit to a new route.	For all OCH circuit types.
Priority	Prioritize the restoration operation for the failed OCH circuit. Values are High, Priority 1, Priority 2, Priority 3, Priority 4, Priority 5, Priority 6, and Low.	For all OCH circuit types when the Restoration check box is checked.
Restoration Validation	Validation mode for the restoration operation. Values are: <ul style="list-style-type: none"> <li>• None—The circuit is restored without considering the restoration acceptance threshold value.</li> <li>• Inherited— The restoration circuit inherits the validation and acceptance threshold values from the primary circuit.</li> <li>• Full—The circuit is restored when the restoration validation result is greater than or equal to the restoration acceptance threshold value.</li> </ul>	For all OCH circuit types when the Restoration check box is checked.
Restoration Acceptance Threshold	Acceptance threshold value set for the restoration operation for OCH circuits. Values are: <ul style="list-style-type: none"> <li>• Green—Indicates that the restoration failure risk is 0%.</li> <li>• Yellow—Indicates that the restoration failure risk is between 0% and 16%.</li> <li>• Orange—Indicates that the restoration failure risk is between 16% and 50%.</li> <li>• Red—Indicates that the restoration failure risk is greater than 50%.</li> </ul>	For all OCH circuit types when: <ul style="list-style-type: none"> <li>• Restoration check box is checked.</li> <li>• Restoration Validation field is set to Full.</li> </ul>

Attribute	Description	Enabled
Restoration Protect Acceptance Threshold	Protection acceptance threshold value set for the restoration operation for OCH protected circuits. Values are: <ul style="list-style-type: none"> <li>• Green—Indicates that the restoration failure risk is 0%.</li> <li>• Yellow—Indicates that the restoration failure risk is between 0% and 16%.</li> <li>• Orange—Indicates that the restoration failure risk is between 16% and 50%.</li> <li>• Red—Indicates that the restoration failure risk is greater than 50%.</li> </ul>	For OCHNC WSON circuit type when: <ul style="list-style-type: none"> <li>• Protection field is set to PSM, Y-Cable, or Splitter..</li> <li>• Restoration check box is checked.</li> <li>• Restoration Validation field is set to Full.</li> </ul>
Revert	Reverts the circuit from the restored path to the original path after a failure is fixed. Values are None, Manual, and Automatic.	For OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types when the Restoration check box is checked.
Soak Time	Period that the circuit on the restored path waits before switching to the original path after a failure is fixed.	For OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types when Revert is set to Manual or Automatic.
Admin State	Select the admin state of the circuit as <b>Up</b> or <b>Down</b> . This impacts the circuit's operability and determines whether the circuit can be activated or deactivated.	For OCH-Trail UNI circuit type.
<b>Preferred Wavelength Properties</b>		
Wavelength Options	Wavelength options for the circuit. Values are <b>Do Not Set</b> , <b>Set To Default</b> , and <b>Set Preferred Wavelength</b> .	For OCH-Trail UNI circuit type.
<b>Work Port Properties</b>		
Auto Provisioning	Check this check box to enable the Auto Provisioning feature.	For all OCH circuit types

Attribute	Description	Enabled
C Band	<p>Conventional wavelength window to provision the circuit. Values are:</p> <ul style="list-style-type: none"> <li>• Odd—The odd position in the ITU grid.</li> <li>• Even—The even position in the ITU grid.</li> </ul>	<ul style="list-style-type: none"> <li>• For all OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types when the Auto Provisioning check box is unchecked.</li> <li>• For OCH-Trail UNI circuit type when the Wavelength Options is set to Set Preferred Wavelength.</li> </ul>
Wavelength/Frequency	<p>Wavelength or frequency of the circuit. This value is applicable for the C Band that you chose.</p> <p><b>Note</b> You must set the DWDM grid unit to either wavelength or frequency. To do this, go to <b>Administration &gt; Settings &gt; System Settings &gt; Circuits/VCs Display</b>, and under the DWDM Grid Unit area, choose either <b>Wavelength (Nanometer (nm))</b> or <b>Frequency (Terahertz (THz))</b>.</p>	For all OCH circuit types when the C Band field is set to Odd or Even.
Preferred/Required	Select to determine whether the values set in the C Band and Wavelength/Frequency fields are preferred or required to provision the circuit.	For all OCH circuit types when the Auto Provisioning check box is unchecked.
<b>Protect Port Properties</b>		
Copy from Work Port	Check this check box to copy the values set in the Work Port Properties section.	For all OCH circuit types when the Protection field is set to PSM, Y-Cable, or Splitter.

## Create and Provision Two Mutually Diverse OCH-Trail UNI Circuits

Use this procedure to create two OCH-Trail UNI circuits that are mutually diverse from each other. Both the circuits must originate from the same device. You can create both the circuits quickly using the Provisioning wizard in a single workflow .

### Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see [Prerequisites for Provisioning Optical Circuits, on page 448](#).

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click **Device Groups**, and then select the location in which you want to create the OCH circuit.
- Step 3** Close the **Device Groups** popup window.
- Step 4** In the **Network Topology** window, click **Circuits/VCs**.
- Step 5** Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.
- You can also access the Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.
- Step 6** From the **Technology** drop-down list, choose **Optical**.
- Step 7** In the **Service Type** area, choose **OCH-Trail UNI**.
- Step 8** If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles , on page 509](#).
- Step 9** Click **Next** to go to the **Customer Section** page.
- Step 10** Check the **Mutual Diversity** check box to create two OCH-Trail UNI circuits that are mutually diverse from each other.
- Step 11** Enter the circuit name and its description in the **Customer Section** page.
- Step 12** Click **Next** to go to the **Endpoint Section** page.
- Step 13** Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Interface.
- Note** When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.
- Step 14** Click **Next** to go to the **Circuit Section** page.
- Step 15** Enter the circuit details. See [Circuit Section Reference for OCH Circuit Types, on page 450](#) for descriptions of the fields and attributes.
- Step 16** Click **Next** to go to the **Constraints Section** page.
- Step 17** Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.
- Note** When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.
- Step 18** Click **Next**. The **Customer Section** page for the second circuit is displayed.
- Step 19** Repeat Step 11 to Step 17 to create the second circuit.
- Step 20** Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it but you cannot edit the attributes.
- Step 21** The circuits should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC names to see the Circuit/VC 360 view.
-

# Create and Provision a Media Channel Group SSON Circuit

To create and provision a Media Channel Group SSON circuit:

## Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see [Prerequisites for Provisioning Optical Circuits, on page 448](#).

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click **Device Groups**, and then select the location in which you want to create the Media Channel Group SSON circuit.
- Step 3** Close the **Device Groups** popup window.
- Step 4** In the **Network Topology** window, click **Circuits/VCs**.
- Step 5** Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.
- You can also access the Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.
- Step 6** From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area.
- Step 7** In the **Service Type** area, choose **Media Channel Group SSON**.
- Step 8** If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles, on page 509](#).
- Step 9** Click **Next** to go to the **Customer Section** page.
- Step 10** (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.
- Step 11** Enter the circuit name and its description in the **Customer Section** page.
- Note** A maximum of only 80 characters are allowed for the Circuit Name field.
- Step 12** Click **Next** to go to the **Endpoint Section** page.
- Step 13** Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name, Termination Point, and Add/Drop Port columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.
- Note** When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.
- Step 14** Click **Next** to go to the **Circuit Section** page.
- Step 15** Choose the required circuit width.
- Step 16** To set the **Central Wavelength/Frequency Properties**, do one of the following:
- Check the **Auto Provisioning** check box.
  - Choose the required **Wavelength** for the circuit and then choose either **Preferred** or **Required** option to determine whether the values set in the **Wavelength** field is preferred or required to provision the circuit.
- Step 17** Click **Next** to go to the **Constraints Section** page.

**Step 18** Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

**Note** When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

**Step 19** Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

---

The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

## Create and Provision a Media Channel SSON Circuit

To create and provision a Media Channel SSON circuit:

### Before you begin

- Ensure that a Media channel group SSON is already created to associate the Media Channel SSON circuits with the Media channel group. See [Create and Provision a Media Channel Group SSON Circuit, on page 456](#).
- For information about the prerequisites that must be met before you can provision an optical circuit, see [Prerequisites for Provisioning Optical Circuits, on page 448](#).

---

**Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.

**Step 2** Click **Device Groups**, and then select the location in which you want to create the Media Channel SSON circuit.

**Step 3** Close the **Device Groups** popup window.

**Step 4** In the **Network Topology** window, click **Circuits/VCs**.

**Step 5** Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.

**Step 6** From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, optical service types for Media Channel SSON circuits include Media Channel NC SSON, Media Channel Trail SSON, and Media Channel CC SSON.

**Step 7** In the **Service Type** area, choose the type of Media Channel SSON circuit you want to create.

**Step 8** If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles , on page 509](#).

**Step 9** Click **Next** to go to the **Customer Section** page.

**Step 10** (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.

**Step 11** Enter the circuit name and its description in the **Customer Section** page.

**Note** For the Media Channel NC SSON and Media Channel Trail SSON circuits, a maximum of only 77 characters are allowed in the Circuit Name field. Of the 77 characters, three characters are reserved for carrier suffix.

For the Media Channel CC SSON circuits, a maximum of 71 characters are allowed in the Circuit Name field.

**Step 12** Click **Next** to go to the **Endpoint Section** page.

**Step 13** Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Termination Point columns. The Side column gets auto-populated based on the termination point selected. Only network elements that are available and compatible with the circuit type you chose will be displayed.

**Note** The MCH-Trail Name column is available only when you create a Media Channel CC SSON circuit.

**Step 14** Select a media channel diversity for the MCH circuit. The MCH circuit that you are creating will be diverse from the media channel that you choose.

**Note** You cannot modify or delete the media channel diversity once it is created.

**Step 15** Click **Next** to go to the **Circuit Section** page.

**Note** For the Media Channel CC SSON circuits, the **Circuit Section** page is not available if you have entered an MCH-Trail Name in the Endpoints table.

**Step 16** Choose the Media Channel Group to which you want to associate the Media Channel SSON circuit.

**Step 17** Enter the circuit details. See [Circuit Section Reference for Media Channel SSON Circuit Types, on page 458](#) for descriptions of the fields and attributes.

**Step 18** Click **Next** to go to the **Constraints Section** page.

**Step 19** Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

**Note** When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

**Step 20** Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

---

The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

## Circuit Section Reference for Media Channel SSON Circuit Types

The following table lists and describes the attributes that define the Media Channel SSON circuit types.

**Table 32: Circuit Section Reference—Media Channel SSON Circuit Types**

Attribute	Description	Enabled
Central Wavelength/Frequency Properties		



Attribute	Description	Enabled
Auto Provisioning	Check this check box to automatically set the wavelength or frequency properties for the circuit.	For all Media Channel SSON circuit types.
Wavelength (nm)	<p>Wavelength or frequency of the circuit.</p> <p><b>Note</b> You must set the DWDM grid unit to either wavelength or frequency. To do this, go to <b>Administration &gt; Settings &gt; System Settings &gt; Circuits/VCs Display</b>, and under the DWDM Grid Unit area, choose either <b>Wavelength (Nanometer (nm))</b> or <b>Frequency (Terahertz (THz))</b>.</p>	For all Media Channel SSON circuit types when the Auto Provisioning check box is unchecked.
Preferred/Required	Select to determine whether the values set in the Wavelength field is preferred or required to provision the circuit.	For all Media Channel SSON circuit types when the Auto Provisioning check box is unchecked.
<b>Optical Properties</b>		
Validation	<p>Validation mode for the circuit. Values are:</p> <ul style="list-style-type: none"> <li>• Full—The circuit is created when the circuit validation result is greater than or equal to the acceptance threshold value.</li> <li>• None—The circuit is created without considering the acceptance threshold value.</li> </ul>	For all Media Channel SSON circuit types.
Acceptance Threshold	<p>Protection acceptance threshold value set for the circuit. Values are:</p> <ul style="list-style-type: none"> <li>• Green—Indicates that the restoration failure risk is 0%.</li> <li>• Yellow—Indicates that the restoration failure risk is between 0% and 16%.</li> <li>• Orange—Indicates that the restoration failure risk is between 16% and 50%.</li> <li>• Red—Indicates that the restoration failure risk is greater than 50%.</li> </ul>	For all Media Channel SSON circuit types when the Validation field is set to Full.
Ignore Path Alarms	Check the check box to ignore path alarms.	For all Media Channel SSON circuit types.
Allow Regeneration	Check the check box to allow the network elements to regenerate the signal.	For all Media Channel SSON circuit types.
Restoration	Check this check box to restore the failed Media Channel SSON circuit to a new route.	For all Media Channel SSON circuit types.
Priority	Prioritize the restoration operation for the failed circuit. Values are High, Priority 1, Priority 2, Priority 3, Priority 4, Priority 5, Priority 6, and Low.	For all Media Channel SSON circuit types when the Restoration check box is checked.

Attribute	Description	Enabled
Restoration Validation	Validation mode for the restoration operation. Values are: <ul style="list-style-type: none"> <li>• None—The circuit is restored without considering the restoration acceptance threshold value.</li> <li>• Inherited— The restored circuit inherits the validation and acceptance threshold values from the primary circuit.</li> <li>• Full—The circuit is restored when the restoration validation result is greater than or equal to the restoration acceptance threshold value.</li> </ul>	For all Media Channel SSON circuit types when the Restoration check box is checked.
Restoration Acceptance Threshold	Acceptance threshold value set for the restoration operation for the circuit. Values are: <ul style="list-style-type: none"> <li>• Green—Indicates that the restoration failure risk is 0%.</li> <li>• Yellow—Indicates that the restoration failure risk is between 0% and 16%.</li> <li>• Orange—Indicates that the restoration failure risk is between 16% and 50%.</li> <li>• Red—Indicates that the restoration failure risk is greater than 50%.</li> </ul>	For all Media Channel SSON circuit types when: <ul style="list-style-type: none"> <li>• Restoration check box is checked.</li> <li>• Restoration Validation field is set to Full.</li> </ul>
Revert	Reverts the circuit from the restored path to the original path after a failure is fixed. Values are None, Manual, and Automatic.	For all Media Channel SSON circuit types when the Restoration check box is checked.
Soak Time	Period that the circuit on the restored path waits before switching to the original path after a failure is fixed.	For all Media Channel SSON circuit types when the Revert option is set to Manual or Automatic.

## Create and Provision an OTN Circuit

To provision an OTN circuit:

### Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see [Prerequisites for Provisioning Optical Circuits, on page 448](#).

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click **Device Groups**, and then select the location in which you want to create the OTN circuit.
- Step 3** In the **Network Topology** window, click **Circuits/VCs**.
- Step 4** Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.

- Step 5** From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, service types for OTN circuits include ODU UNI, ODU Tunnel, OPU over ODU, and ODU UNI Hairpin.
- Step 6** In the **Service Type** area, choose the type of OTN circuit you want to create.
- Step 7** If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles](#), on page 509.
- Step 8** Click **Next** to go to the **Customer Details** page.
- Step 9** (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.
- Step 10** Enter the circuit name and its description in the **Customer Details** page.
- Step 11** Click **Next** to go to the **Circuit Details** page.
- Step 12** Enter the circuit details. See [Circuit Section Reference for OTN Circuit Types](#), on page 461 for descriptions of the fields and attributes.
- Step 13** Click **Next** to go to the **Endpoint Section** page.
- Step 14** Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Interface/Termination Point columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.
- Note** When the row is in the edit mode, you cannot click a device in the map to populate the Device Name column.
- Step 15** Enter the protection type and path options for the circuit. See [Endpoint Section Reference for OTN Circuit Types](#), on page 463 for descriptions of the fields and attributes.
- Step 16** Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview**. After seeing the preview of the TL1 or CLI commands, you can either deploy the configurations to the devices or cancel the provisioning operation.

The circuit should be added to the list in the **Circuits/VCs** tab in the **Network Topology** window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

## Circuit Section Reference for OTN Circuit Types

The following table lists and describes the attributes that define the OTN circuit types.

**Table 33: Circuit Section Reference—OTN Circuit Types**

Attribute	Description	Enabled
<b>Circuit Properties</b>		
Bandwidth	Bandwidth required to provision the OTN circuit.  See <a href="#">Table 35: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits</a> for the mapping of values in the Bandwidth, and Service Type fields.	For all OTN circuit types.

Attribute	Description	Enabled
A-End Open Ended	<p>Check this check box to create an open-ended circuit, in which the source end point is connected to an ODU subcontroller, instead of a client payload controller.</p> <p><b>Note</b> Checking this checkbox will not deploy ODU subcontrollers on the Cisco NCS 4000 devices. You must configure the ODU subcontrollers on the Cisco NCS 4000 devices before adding the devices to Cisco EPN Manager . For more information about the open ended ODU UNIs and how to configure ODU subcontrollers on Cisco NCS 4000 devices, see <a href="#">Open Ended ODU UNI, on page 424</a>.</p>	For ODU UNI circuit type when the Bandwidth field is set to ODU0, ODU1, ODU2, or ODU2E.
Z-End Open Ended	<p>Check this check box to create an open-ended circuit, in which the destination end point is connected to an ODU subcontroller, instead of a client payload controller.</p> <p><b>Note</b> Checking this checkbox will not deploy ODU subcontrollers on the Cisco NCS 4000 devices. You must configure the ODU subcontrollers on the Cisco NCS 4000 devices before adding the devices to Cisco EPN Manager . For more information about the open ended ODU UNIs and how to configure ODU subcontrollers on Cisco NCS 4000 devices, see <a href="#">Open Ended ODU UNI, on page 424</a>.</p>	For ODU UNI circuit type when the Bandwidth field is set to ODU0, ODU1, ODU2, or ODU2E.
Service Type	<p>Service types supported for the selected bandwidth.</p> <p>See <a href="#">Table 35: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits</a> for the mapping of values in the Bandwidth and Service Type fields.</p>	For ODU UNI circuit type.
<b>Route Properties</b>		
Bit Rate	Total number of bits per second.	For all OTN circuit types (except ODU UNI Hairpin) when the Bandwidth field is set to ODUFLEX.
Framing Type	<p>The elementary signal of the requested service. Values are:</p> <ul style="list-style-type: none"> <li>• CBR—Constant bit rate.</li> <li>• GFP-F-Fixed—Fixed and frame mapped generic framing procedure.</li> </ul>	For all OTN circuit types (except ODU UNI Hairpin) when the Bandwidth field is set to ODUFLEX.

Attribute	Description	Enabled
Record Route	Check this check box to record the circuit route.	For all OTN circuit types (except ODU UNI Hairpin).

## Endpoint Section Reference for OTN Circuit Types

The following table lists and describes the attributes that define the protection type and path options for OTN circuit types.

**Table 34: Endpoint Section Reference—OTN Circuit Types**

Attribute	Description	Enabled
<b>Endpoints</b>		
Device Name	<p>A end and Z end devices of the circuit.</p> <p><b>Note</b> For ODU UNI Hairpin circuits, both A end and Z end will be the same device but with different termination points.</p>	For all OTN circuit types.
Interface	Interface names for the A end and Z end devices.	For ODU UNI circuits.
Termination Point	Termination point for the cards.	For OPU over ODU and ODU UNI Hairpin circuits.
Protection Type	<p>Protection type for the OTN circuit. Values are:</p> <ul style="list-style-type: none"> <li>1+0—Unprotected card. If a failure is detected in the working path, it results in loss of data.</li> <li>1+1—Both primary and secondary path carry traffic end to end and the receiver receives and compares both the traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path.</li> <li>1+R—When the primary path fails, the restored path is calculated and traffic is switched to the restored path. If the primary path is non-revertible, the restored path becomes the new primary path.</li> <li>1+1+R—Both primary and secondary path carry traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path. The restored path is calculated and traffic is switched to the restored path. If the primary or secondary path is non-revertible, the restored path becomes the new primary or secondary path.</li> </ul> <p><b>Note</b> This protection type is not supported for Cisco NCS 4000 series devices.</p>	For all OTN circuit types (except ODU UNI Hairpin).

Attribute	Description	Enabled
Diverse From Tunnel ID	Select a tunnel to ensure that it is not used by the circuit you are provisioning. This is to ensure that if there is a failure in a tunnel, the same tunnel is not used by another circuit.	For all OTN circuit types(except ODU UNI Hairpin).
<b>Working Path, Protected Path, and Restored Path</b> <p>The Protected Path field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+1 or 1+1+R.</p> <p>The Restored Path field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+R or 1+1+R.</p>		
Type	Choose the type of working path or protected path for the circuit. Values are Dynamic and Explicit.	For all OTN circuit types (except ODU UNI Hairpin).
New	Check this check box to create a new explicit working or protected path for the circuit.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit.
Select Existing EP	Choose an existing explicit working or protected path for the circuit.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit and the New check box is unchecked.
New Name	Enter a name for the explicit path that you are creating. In the table below the New Name field, click the '+' button to add a new row to the table, and then select a device and an explicit path controller as the interface for the device.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit and the New check box is checked.
<b>Protection Profile</b> <p>The Protection Profile field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+1, 1+R, or 1+1+R and a valid A end device is selected.</p>		

Attribute	Description	Enabled
Protection Profile	<p>The profile used to manage the protection of the circuit. This protection profile must be configured on the A end node of the circuit.</p> <p><b>Note</b> You can enter the protection profile that was configured on the device.</p> <p>The details of the protection profile such as the protection type, SNC, hold off, wait to restore, and whether the circuit is revertive are displayed.</p>	

## Bandwidth and Service Type Value Mapping for ODU UNI Circuits.

The following table maps the values in the Bandwidth and Service Type fields for the ODU UNI circuits

**Table 35: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits**

Bandwidth	Service Type
ODU0	<ul style="list-style-type: none"> <li>Ethernet OPU0 GMP</li> </ul>
ODU1	<ul style="list-style-type: none"> <li>OTN OPU1</li> <li>Sonet OPU1 BMP</li> <li>SDH OPU1 BMP</li> </ul>
ODU1E	<ul style="list-style-type: none"> <li>Ethernet OPU1e BMP</li> <li>OTN OPU1e</li> </ul>
ODU1F	<ul style="list-style-type: none"> <li>OTN OPU1f</li> </ul>
ODU2	<ul style="list-style-type: none"> <li>Ethernet OPU2 GFP_F</li> <li>Ethernet OPU2 GFP_F_EXT</li> <li>Ethernet OPU2 WIS</li> <li>OTN OPU2</li> <li>Sonet OPU2 AMP</li> <li>Sonet OPU2 BMP</li> <li>SDH OPU2 AMP</li> <li>SDH OPU2 BMP</li> </ul>
ODU2E	<ul style="list-style-type: none"> <li>Ethernet OPU2e BMP</li> <li>OTN OPU2e</li> </ul>
ODU2F	<ul style="list-style-type: none"> <li>OTN OPU2f</li> </ul>
ODU4	<ul style="list-style-type: none"> <li>OTN OPU4</li> <li>Ethernet OPU4 GFP_F</li> <li>Ethernet OPU4 GMP</li> </ul>
ODUFLEX	<ul style="list-style-type: none"> <li>OTN OPUFlex</li> <li>Ethernet OPUFlex GFP_F</li> </ul>

## Create and Provision an ODU Circuit

To create and provision an ODU circuit:

### Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see [Prerequisites for Provisioning Optical Circuits, on page 448](#).

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click **Device Groups**, and then select the location in which you want to create the ODU circuit.
- Step 3** Close the **Device Groups** popup window.
- Step 4** In the **Network Topology** window, click **Circuits/VCs**.
- Step 5** Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.
- You can also access the Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.
- Step 6** From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area.
- Step 7** In the **Service Type** area, choose **ODU**.
- Step 8** If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles, on page 509](#).
- Step 9** Click **Next** to go to the **Customer Section** page.
- Step 10** (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.
- Step 11** Enter the circuit name and its description in the **Customer Section** page.
- Step 12** Click **Next** to go to the **Circuit Section** page.
- Step 13** Choose one of the following protection type for the circuit:
- **None**—No protection type for the circuit.
  - **1+1**—Both primary and secondary paths carry traffic end to end and. The receiver receives the traffic from both primary and secondary paths, and compares both the traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path.
- Note** If you have selected 1+1 as the protection type, the Connection Mode is set to SNC-N, by default.
- Step 14** Choose the required Reversion Time and Hold off Timer for the circuit.
- Note** These fields are available only if you have selected 1+1 as the protection type.
- Step 15** Click **Next** to go to the **Endpoint Section** page.
- Step 16** Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Termination Point columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.
- Note** When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.
- Step 17** Click **Next** to go to the **Constraints Section** page.



**Step 18** Click a device node in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements that are compatible with the ODU circuit type will be displayed.

**Note** You cannot provide links as constraints for ODU circuits.

**Step 19** (Optional) Click **Calculate Path** to verify if there is a valid working path between the selected endpoints. If a valid working path exists between the selected endpoints, the path appears with a 'W' label on the topology map. If a valid working path does not exist between the selected endpoints, a Path Calculation Result section appears that displays the reason why a working path cannot be established between the selected endpoints.

**Step 20** Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

---

The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

## Provision L3VPN Services

- [Supported L3VPN Services, on page 427](#)
- [L3VPN Provisioning Features and Limitations, on page 468](#)
- [Prerequisites for L3VPN Provisioning , on page 469](#)
- [L3VPN Service Discovery , on page 470](#)
- [Create and Provision a New L3VPN Service, on page 471](#)
- [View L3VPN Service Details, on page 481](#)
- [Modify L3VPNs and VRFs, on page 481](#)
- [Add and Copy VRFs to an L3VPN Service, on page 482](#)
- [Example Configuration: Provisioning an L3VPN Service, on page 479](#)

## Supported L3VPN Services

An MPLS Layer 3 VPN creates a private IP network. The customer connects to the network via customer edge (CE) routers, which act as IP peers of provider edge (PE) routers.

### Virtual Routing and Forwarding (VRFs)

On the PE, Virtual Routing and Forwarding (VRF) instances act as virtual IP routers dedicated to forwarding traffic for the L3VPN service. The VRFs learn the routes to each other via the Multi-Protocol Border Gateway Protocol (MP-BGP), and then forward traffic using MPLS.

A VPN is comprised of at least one but typically several VRFs. Cisco EPN Manager uses the VPN ID to discover which VRFs together form a single VPN. If Cisco EPN Manager discovers an existing network where no VPN ID has been provisioned, it takes all VRFs with the same name and associates them into one VPN. For VPNs created using Cisco Prime Provisioning, which uses a naming convention with version number

prefixes and different suffixes, Cisco EPN Manager will recognize the different VRFs as belonging to one VPN.

In general there is a regular expression which can be configured to allow for varying naming convention.

### Route Targets (RTs)

The connections between VRFs are defined using Route Targets (RTs) that are imported and exported by the VRFs. Cisco EPN Manager makes it easy to set up a full mesh of connections, and automatically allocates the route target to be used. The route target consists of a prefix which is either an AS number or an IPv4 address, for example, a full mesh prefix, 100 [681682]. The prefix can be selected from the existing BGP autonomous system (AS) numbers in the network, or it can be entered manually. The second number following the prefix is allocated automatically by Cisco EPN Manager.

Alternatively or in addition to the full mesh, it is possible to manually select route targets. During VPN creation, there is an initial screen where you type in the route targets to be used within a VPN, and then for each VRF you can select which route targets you import and export. You also specify for which address family (IPv4 or IPv6) you will use the route target. This can be used for example to configure extranets, by importing route targets used in other VPNs.

### Route Redistribution

The routes that are exchanged between the PE and the CE have to be redistributed into the MP-BGP routing protocol so that remote endpoints can know which prefixes can be reached at each VRF. To control route redistribution, Cisco EPN Manager allows you to define the required protocol (Static, Connected, or RIP), the protocol's metric value, and optionally the applicable route policy.

### Endpoints

Cisco EPN Manager supports the creation of IP endpoints on Ethernet subinterfaces. It supports selecting untagged encapsulation, or specifying an outer and optionally an inner VLAN, with 802.1q or 802.1ad encapsulation. You can specify both IPv4 and Ipv6 addresses at an endpoint. You can also specify the BGP and OSPF neighbor details to provision BGP and OSPF neighbors between CE and PE.

For information on how to provision L3VPN service using Cisco EPN Manager, see, [Provision L3VPN Services, on page 467](#).

## L3VPN Provisioning Features and Limitations

**Cisco EPN Manager supports the following L3VPN features:**

- Creation of VRFs.
- Automatic allocation of VPN IDs and Route Target IDs.
- Automatic allocation of route distinguishers.
- Discovery of VPNs consisting of several VRFs, based on multiple criteria (VPN ID, common name, and Prime Provisioning naming conventions).
- You can select devices for L3VPN provisioning using the Point and Click method of provisioning.
- Definition of IP endpoints attached to a VRF. Associating Ethernet subinterfaces with VRFs.
- Provisioning of BGP OSPF neighbors between CE and PE.
- Attaching QoS profiles to the endpoint interfaces.
- Adding new VRFs to existing VPNs.

- Modifying VPNs and associated VRFs created and deployed (or discovered and promoted) using Cisco EPN Manager .
- Overlays in the Network Topology for L3VPN services.
- Promotion of L3VPN services discovered directly from the device. This further helps in modifying and deleting discovered services.
- Using route targets with OSPF dual AS routing.
- Using integrated routing and bridging to provision L3VPN services using BDI/BVI interfaces (subinterfaces).
- Associating IP Service Level Agreements (SLAs) and CLI templates with L3VPN services.
- Route redistribution between the PE-CE link and the MP-BGP core using connected, static, RIP, or OSPF routes.
- Provisioning L3VPN services using LAG interfaces.

**Cisco EPN Manager has the following L3VPN limitations:**

- VRFs are supported only on Cisco ASR1000, Cisco ASR9000, Cisco ASR90X, Cisco ASR 920X, and Cisco ASR901S devices.
- You cannot provision multicast VPNs. Only unicast VPNs are supported.
- While creating the L3VPN service, you can add only up to five VRFs to the VPN. More VRFs can later be added to the VPN using the Modify VRF and Add VRF options.
- Only one VRF per device is supported. You can create multiple VRFs but on different devices either with the same VRF name or with different VRF names.
- Route policies can be selected but cannot be defined within the L3VPN service.
- Only BGP and OSPF PE-CE routing protocol is supported.
- There is no support for multiple attached PEs, and so there is no Site of Origin and HSRP support.
- IP SLA operations can be associated with VRFs only during service creation and not during service modification.
- Deleting an L3VPN service deletes the IP SLA operations associated with the service from the device. And the associated operations that are deleted will not be available for future usage.
- The Integrated Routing and Bridging (IRB) is not supported for Cisco Catalyst 6500 series switches..

## Prerequisites for L3VPN Provisioning

For more information about implementing L3VPNs, see [Implementing MPLS Layer 3 VPNs](#).

Before you begin provisioning L3VPN services, ensure that the following pre-requisites are followed.

Following are the prerequisites for provisioning an L3VPN service:

- BGP must be set up on all devices. Typically all devices must communicate with each other via a pair of route reflectors.
- Pre-configuration changes required to set up BGP:

Configure the BGP router-id as shown in the example below:

```
router bgp 65300
  bgp router-id 1.1.1.1
```

Set Vpn4 and Vpn6 as the parent address family using these commands:

```
router bgp 100
  address-family vpnv4 unicast
  address-family vpnv6 unicast
```

- MPLS reachability must be set up between the devices. MPLS core network configuration must be set up.
- Inventory collection status for the devices on which the L3VPN services will be provisioned must be 'Completed'. To check the status of devices, go to **Inventory > Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
- (Optional) Customers must be created in the system so that you can associate the L3VPN service to a customer during L3VPN service provisioning. To create and manage customers, choose **Inventory > Other > Customers**.

## L3VPN Service Discovery

Cisco EPN Manager associates multiple VRFs into a single VPN using multiple criteria:

- If VRFs were configured with a VPN ID: then the VPN service is discovered using the VPN ID to identify the VRFs that belong to the same VPN. If you have VPNs that you need to discover, where different VRF names are used within one VPN, then Cisco EPN Manager discovers the VRFs by the VRF names.

In cases where no more than one VRF is created per device, it is common practice to simply use the same VRF name everywhere across the VPN. If Cisco EPN Manager sees multiple VRFs with the same name and no VPN ID, then it considers them as a single VPN, and the VPN name will be the name of the VRFs.

- If VPNs that were originally provisioned using Prime Provisioning: Cisco EPN Manager is also aware of the Prime Provisioning VRF naming convention. The naming convention used by Prime Provisioning is in the format:

V<number>:<VPN name><optional suffix, one of -s -h -etc>

VRFs with the same names and numbers will belong to the same VPN. For example these are VRFs belonging to a VPN called 'ABC':

V1:ABC, V2:ABC, V4:ABC-s, V22:ABC-h, V001:ABC, etc.

- If the VRF has no VPN ID: and has a unique name that doesn't match other names according to the Prime Provisioning convention, it will be placed into a VPN on its own. The name of the VPN will be the name of the VRF.

The Prime Provisioning naming convention feature is driven by a regular expression that is embedded in the product. If configuring a VPN is not an option for you and you have a naming convention that could be matched with a regular expression, it is possible to change it. To change the regular expression, please contact your Cisco Advanced Services representative.

## Create and Provision a New L3VPN Service

The process of creating and provisioning a unicast L3VPN involves:

- (Optional) Associating a customer to the VPN.
- Defining the attributes that influence how traffic that is delivered over the L3VPN and through its endpoints will be treated.
- Specifying the endpoints and route redistribution values of the L3VPN.
- (Optional) Configuring IP Service Level Agreements (SLAs) operation to monitor end-to-end response time between devices using IPv4 or IPv6.
- (Optional) Associating user defined CLI templates with the L3VPN service.

Note: Only Unicast L3VPN services are supported in this release.

To create a new L3VPN service:

---

**Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.

The network topology window opens.

**Step 2** From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.

**Step 3** Click the **Circuits/VCs** tab, then click the + (**Create**) icon in the **Circuits/VCs** pane toolbar.

The Provisioning Wizard opens in a new pane to the right of the map. You can also access the L3VPN Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.

**Step 4** From the **Technology** drop-down list, select **L3VPN**. A list of supported L3VPN service types is displayed.

**Step 5** In the **Service Type** section, choose **Unicast** and click **Next** to enter the customer and service details. In this release, only service type Unicast L3VPN is supported.

**Step 6** (Optional) Select the customer that you want to associate with the VPN. If there are no customers in the drop-down list, you can go to **Inventory > Other > Customers** to create the customer and return to this step.

**Step 7** Specify the basic L3VPN parameters:

- a) Use the **Activate** check box to specify whether the service must be in active (check box enabled) or inactive (check box disabled) state. The Active state enables traffic to pass through the circuit and automatically sets the Service State for all associated IP endpoints to True. In the Inactive state, you can choose to set the service state for IP endpoints to true or false.
- b) Provide a unique name for the service and optionally enter a description
- c) In the **IP MTU** field, enter a value between 1522 (default) and 9216. The service MTU is the size in bytes of the largest IP packet that can be carried unfragmented across the L3VPN. It does not include layer 2 headers.

The configured interface MTU is the service MTU plus the size of any layer 2 headers. For Ethernet, this will add 14 bytes plus 4 bytes per VLAN header.

The value of the UNI MTU depends on the service MTU and outer and inner VLAN values:

- If both outer and inner VLANs are present, then the UNI MTU value is greater than the Service MTU + 14 + (4\*2)
- If only the outer VLAN is present, then the UNI MTU value is greater than the Service MTU + 14 + (4 \*1)
- If no VLANs are present, then the UNI MTU value is greater than the Service MTU + 14

- d) (Optional) To create a full mesh topology for this service, select the **Create Full Mesh** check box and enter the full mesh prefix manually in the **New Prefix** field or select a value from the **Existing Prefix** drop-down list. The available options depend on the full mesh prefix values discovered from the selected device.
- e) Select the address family as **IPv4**, **IPv6**, or **Both** from the **Full Mesh Address Family** drop-down list.

**Step 8** Use the **Route Target Allocation** section to manually specify the route target address families (**IPv4**, **IPv6**, or **Both**) and their associated route target values. You can create multiple route targets for the L3VPN service. These route targets can be associated with any VRF that you attach to this L3VPN service in the following steps.

**Note** The route targets associated with a VRF must also be associated with the L3VPN the VRFs belong to.

**Step 9** In the **Deployment Action** drop-down menu, specify the task that must be taken up when the service creation process is completed. Your options are:

- **Preview**: allows you to review the configuration that is generated before it is deployed to the device.
- **Deploy**: allows you to deploy the configuration to the relevant devices immediately upon completion.

**Step 10** Click **Next** to associate VRFs to the L3VPN service.

**Step 11** Select the required VRFs from the **VRFs** drop-down list or add a new VRF as explained below, and then click **Next**. During L3VPN service creation, you can associate up to five VRFs with the VPN. To associate more VRFs to the VPN, see [Add and Copy VRFs to an L3VPN Service, on page 482](#). To create a new VRF:

1. Click the '+' icon to add the VRF details manually. To auto populate the VRF details, click the respective device on the map. The device details and a new name for the VRF are automatically populated on the Add VRFs page.
2. To manually specify the VRF details, select the required device from the **Device** drop-down list. You can then manually enter the VRF name and description, and check the **RD Auto** check box.

**Note** If multiple VRFs are created on the same device, you must name them differently to ensure that they are not part of the same VPN. You cannot create multiple VRFs with the same names on the same device.

**Step 12** Specify the IPv4 and IPv6 route targets and route distribution details:

1. **Route Targets**: Select the route targets for this VRF from the **Route Target** drop-down menu. The options in this drop-down menu are available based on the route targets associated with this service in Step 7.
2. Select the direction in which the route targets must be applied. Depending on the device you select, choose **Import**, **Export**, **Both**, or **None**.

Choose the directions depending on the type of device that is selected. For example, for Cisco IOS-XR devices, you cannot choose 'None' as the route target direction.

3. In the **Route Policy** section, select the import and export policy for the route targets.
4. In the **Route Distribution** section, specify the protocol that must be associated with the VRF, the protocol's metric value, the routing process ID, the relevant route policies and the route match type.
  - **Protocol**- Choose the source protocol from which routes must be redistributed. Your options are Static, Connected, RIP, and OSPF.
  - **Metric**- (Optional) Enter a numeric value for the metric which is used when redistributing from one routing process to another process on the same router.
  - **Routing Process ID**- (applicable only to OSPF and RIP) Specify the unique numerical value that identifies the instance of the routing process on the device.

- **Route Policy-** (Optional) Select one of the route policies present on the selected device. You cannot create route policies using Cisco EPN Manager .
- **Route Match Type** (applicable only to OSPF)- Specify the match type that must be associated with the selected route policy. Your options are: Internal, External, External 1, External 2, NSSA External, NSSA External 1, NSSA External 2, NSSA, Level 1, Level 2, and Level Inter Area.

**Step 13** Specify the IP endpoints and UNIs values manually as follows:

- If the endpoint interface has already been configured as a UNI, uncheck the **New UNI** check box and select the required UNI from the **UNI Name** drop-down list.
  - To create a new UNI:
    1. Select the **New UNI** check box.
    2. In the **UNI Name** field, enter a unique name for the UNI.
    3. In the **Device** drop-down, select the device, its required interface, and provide a description for the UNI.
    4. Check the **Service Multiplexing** check box to enable more than one L3VPN or Carrier Ethernet service to be supported at the UNI.
    5. Specify the IP Maximum Transmission Unit (MTU) for the UNI., the speed and duplex settings for the UNI.
    6. Either check the **Auto Negotiation** check box to automatically adjust the speed and duplex settings for the UNI or uncheck the **Auto Negotiation** check box and specify the speed and duplex settings manually.
    7. Choose the UNI QoS profiles for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. If you select a UNI QoS profile, you cannot add individual QoS policies to the service endpoint in the upcoming steps. If you want to add specific QoS policies to the endpoint, leave the UNI Ingress and Egress QoS Profile fields blank.
- Note** You can choose two different discovered QoS profiles for the ingress and egress directions, however, in case of user defined QoS profiles, only a single QoS profile can be chosen for both directions.
8. Select **Enable Link OAM** to enable IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this UNI and the customer's access switch.
  9. Select **Enable Link Management** to enable the customer access switch to get information about this UNI, VLAN IDs, services on the UNI, and so on.

For a detailed description of the fields and attributes in the UNI table, see [New UNI Details Reference, on page 442](#).

**Step 14** Specify the service end point to be associated with the L3VPN by providing the following details, and then click **Next**:

- **VRF Name:** Choose one of the available VRFs that can be associated with this VPN.
- **IPv4 and IPv6 address:** Enter the IP addresses and network masks of the service end point. The masks can be entered simply as an integer that represents the length of the network mask (or in CIDR format).
- **VLAN and Inner VLAN:** Enter the inner and outer VLAN identifiers using integers between 1 and 4094. Inner VLAN is the identifier for the second level of VLAN tagging.

- **QoS Policy:** (Optional) Select the QoS policy that must be applied to the service endpoint. This field is disabled if you have associated UNI Ingress/Egress QoS profiles to the service in the above step. For information on creating QoS profiles, see [Configure Quality of Service \(QoS\)](#) , on page 369.

**Note** You can choose two different discovered QoS policies for the ingress and egress directions, however, in case of user defined QoS policies, only a single QoS policy can be chosen for both directions.

- **Service State:** Specify whether the service state for associated IP endpoints must be set to true or false. If the L3VPN is in Activate state (specified in Step 6 above), this check box is disabled and all service state values are automatically set to True.

- **Use Integrated Routing & Bridging:** Specify whether the VRF and IP addresses must be configured under the sub-interfaces or under the BVI (virtual) interfaces.

**Note** This check box is enabled only when you select devices such as, Cisco ASR 90XX devices, that support integrated routing and bridging.

**Step 15** Click **Next** to go to the **PE-CE Routing** page.

**Step 16** Click the '+' icon to add the PE-CE routing details. See [PE-CE Routing Details References](#), on page 478.

**Step 17** (Optional) Select existing IP SLA parameters from the list, or specify the IP SLA operation parameters described in the table below and then click **Next**.



IP SLA Settings	IP SLA Parameters	Descriptions
Operation Settings	Name	Enter a unique name to identify the IP SLA operation for the selected L3VPN service.
	Type	<p>Select the type of IP SLA operation that must be generated for the devices participating in this L3VPN service. Your options are:</p> <ul style="list-style-type: none"> <li>• <b>UDP Echo:</b> Configures an IP SLAs User Datagram Protocol (UDP) Echo operation to measure response times and to test end-to-end connectivity between a Cisco device and devices using IPv4 or IPv6.</li> <li>• <b>ICMP Echo:</b> Allows you to measure end-to-end network response time between a Cisco device and other devices (source and destination values, as described below) using IPv4 or IPv6. With an IP SLA operation of type ICMP Echo, you cannot associate the 'Connection Loss' action variable.</li> <li>• <b>ICMP Jitter:</b> Configures the Internet Control Message Protocol (ICMP) Jitter operation which provides the capability to generate a stream of ICMP packets between a Cisco IOS device (source) and any other IP device (destination) to gather network performance-related statistics. Statistical measurements for the IP SLAs ICMP jitter operation include latency, round-trip time, jitter (interpacket delay variance), and packet loss.</li> <li>• <b>UDP Jitter:</b> Configures the UDP jitter operation which analyzes round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic in IPv4 or IPv6 networks.</li> </ul>
	Source	Specify the device which acts as the source point from which the IP SLA configuration is generated. The IP SLA responses are generated based on the connectivity between this source device and the target device. The VRF values for this operation are automatically selected based on your Source selection.
	Source Port	Enter a numeric value between 0 and 65535 to specify the source port value for which the IP SLA operation must be configured.
	Destination	Specify the device which acts as the target point from which the IP SLA configuration is generated. The IP SLA responses are generated based on the connectivity between the source device and this target device.
	Destination Port	Enter a numeric value between 0 and 65535 to specify the destination port value for which the IP SLA operation must be generated.
	VRF	The VRF details are automatically selected based on the device you specify as the IP SLA operation Source.

IP SLA Settings	IP SLA Parameters	Descriptions
Reaction Settings	Action Variable	<p>Select the variable based on which the IP SLA reactions must be triggered. For example, when a monitored value exceeds or falls below a specified level, or when a monitored event (such as a timeout or connection loss) occurs.</p> <ul style="list-style-type: none"> <li>• <b>Connection Loss:</b> Indicates that an event must be triggered when a connection loss occurs. This value is not displayed if you select ICPM Echo as the type of operation.</li> <li>• <b>Round Trip Time:</b> If you choose this action variable, you need to enter the <b>Upper Threshold Value</b> and the <b>Lower Threshold Value</b> which indicates that an event must be triggered when a monitored value exceeds or falls below the upper and lower threshold values that you specify.</li> <li>• <b>Time Out:</b> Indicates that an event must be triggered after a given set of consecutive timeouts occur.</li> <li>• <b>Verify Error:</b> Indicates that an event must be triggered after an error of type 'VerifyError' occurs.</li> </ul>
	Action Type	<p>Select one of the following actions that must be taken based on the conditions set in the Action Variable field:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> No action is taken.</li> <li>• <b>Trap and Trigger:</b> Triggers both an SNMP trap and starts another IP SLAs operation when the violation conditions are met, as defined in the Trap Only and Trigger Only options below.</li> <li>• <b>Trap Only:</b> Sends an SNMP logging trap when the specified violation type occurs for the monitored element.</li> <li>• <b>Trigger Only:</b> Changes the state of one or more target operation's Operational state from 'pending' to 'active' when the violation conditions are met. A target operation will continue until its life expires (as specified by the target operation's configured lifetime value). A triggered target operation must finish its life before it can be triggered again.</li> </ul>
	Threshold Type	

IP SLA Settings	IP SLA Parameters	Descriptions
		<p>Select the threshold type based on which the IP SLA events are generated.</p> <ul style="list-style-type: none"> <li>• <b>Average:</b> If you choose this threshold type, enter the <b>N Value</b> which specifies that an event must be triggered when the averaged total value of N probes is reached either when specified upper-threshold value is exceeded, or when it falls below the lower-threshold value.</li> <li>• <b>Consecutive:</b> If you choose this threshold type, enter the <b>Consecutive Values</b> as part of the reaction settings. This threshold type triggers an event only after a violation occurs a specified number of times consecutively. For example, if you enter 5 as the consecutive value, the consecutive violation type is used to configure an action to occur after a timeout occurs 5 times in a row, or when the round-trip-time exceeds the upper threshold value 5 times in a row.</li> <li>• <b>Immediate:</b> Triggers an event immediately when the value for a reaction type (such as response time) exceeds the upper threshold value or falls below the lower threshold value, or when a timeout, connection loss, or verify error event occurs.</li> <li>• <b>Never:</b> Never triggers an event.</li> <li>• <b>X out of Y occurrences:</b> If you choose this threshold type, enter the <b>X Values</b> and <b>Y Values</b> to specify the number of occurrences. This triggers an event after some number (x) of violations within some other number (y) of probe operations (x of y).</li> </ul>
Simple Schedule	-	<p>Enter the scheduling parameters for an individual IP SLAs operation by entering the following values:</p> <ul style="list-style-type: none"> <li>• <b>Frequency:</b> Enter the elapsed time within which the operation must repeat, in seconds.</li> <li>• <b>Life Time:</b> Enter the overall time until when the operation must be active, in seconds. A single operation repeats at the specified frequency for the lifetime of the operation.</li> <li>• <b>Age Out:</b> Enter the length of time to keep an operation active, in seconds. For example, an age out value of 43200 will ensure that the operation will age out after 12 hours of inactivity.</li> <li>• <b>Start Now and Start After:</b> Enable the Start Now check box to schedule the IP SLA operation to be executed immediately on Save. Or use the Start After field to specify the number of minutes after which the operation can be executed.</li> </ul>

**Step 18** (Optional) Use the Service Template page to append a template with additional CLI commands that will be configured on the devices participating in the service. See [Extend a Circuit/VC Using Templates, on page 512](#) for more information.

**Step 19** When you have provided all the required information for the service, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the L3VPN attributes. Otherwise, the configurations will be deployed to the devices immediately.

In case of a deploy failure on even a single device that is part of the service, the configuration is rolled back on all devices participating in the service. To delete the endpoints associated with the service, see, [Delete an L3VPN Service Endpoint, on page 548](#). To add more VRFs to this L3VPN service, see [Add and Copy VRFs to an L3VPN Service, on page 482](#).

## PE-CE Routing Details References

The following table lists and describes the attributes that define the PE-CE details for provisioning a Layer 3 VPN service.

**Table 36: PE-CE Routing Reference**

Attribute	Description
<b>Routing Protocol Settings</b>	
PE Device	Name of the pseudowire device.
VRF	The VRF name that you specified in the VRF page of the wizard is populated.
Routing Protocol Type	Choose either <b>BGP</b> or <b>OSPF</b> as the routing protocol for the Layer 3 VPN service.  <b>Note</b> Based on the routing protocol chosen, either the <b>BGP Neighbor Information</b> section or the <b>OSPF Process Information</b> section will be displayed.
Address Family	Choose the address family as IPv4 or IPv6.  <b>Note</b> IPv6 is not supported for the OSPF routing protocol.
Authentication Type	Choose the authentication type. Only the MD5 authentication type is supported.  <b>Note</b> Authentication Type field is available only when you select OSPF as the routing protocol.
<b>BGP Neighbor Information</b>	
<b>Note</b> This section is available only when you select BGP as the routing protocol.	
Neighbor Address	Enter the IP address of the neighbor.
Neighbor AS	Enter the autonomous system number of this neighbor, which is the unique identifier used to establish a peering session with a BGP neighbor.
Ingress Route Policy	Enter the route policy applied to any BGP routes received from this neighbor.
Egress Route Policy	Enter the route policy applied to any routes sent to this neighbor.
Local AS	Enter the unique local identifier used to establish a peering session with a BGP neighbor.

Attribute	Description
AS Action	<p>Select one of the following action types that must be associated with the local autonomous-system (AS) number:</p> <ul style="list-style-type: none"> <li>• <b>Prepend:</b> Use this option to configure BGP such that it prepends the AS number to routes received from the neighbor.</li> <li>• <b>No Prepend:</b> Use this option to configure BGP such that it does not prepend the AS number to routes received from the neighbor.</li> <li>• <b>No Prepend, Replace AS:</b> Use Replace AS to prepend only the local AS number (as configured with the ip-address) to the AS_PATH attribute. The AS number from the local BGP routing process is not prepended.</li> <li>• <b>No Prepend, Replace AS, Dual AS:</b> Use the Dual AS option to configure the eBGP neighbor to establish a peering session using the AS number (from the local BGP routing process) or by using the AS number configured with the ip-address argument (local-as).</li> </ul>
<b>OSPF Process Information</b>	
<b>Note</b> This section is available only when you select OSPF as the routing protocol.	
Router ID	Specify an IPv4 address for the OSPF protocol.
Area ID	Define an area for the OSPF protocol. The valid range is 0 - 4294967295.
Domain Type	Select the required domain type.
Domain Value	Enter the domain value in the 6 Octet Hexadecimal format. For example, 00000000000F.
BFD Min Interval	<p>Enter the minimum interval between which control packets are sent to the neighbor. The range is between 3 milliseconds and 30000 milliseconds.</p> <p><b>Note</b> This field is available only for Cisco IOS-XR devices.</p>
BFD Multiplier	<p>The multiplier is the number of times a packet is missed before BFD declares the neighbor down. The range for the OSPF protocol is 2 to 50.</p> <p><b>Note</b> This field is available only for Cisco IOS-XR devices.</p>
BFD Fast Detect	<p>Check this check box to quickly detect failures in the path between adjacent forwarding engines.</p> <p><b>Note</b> This field is available only for Cisco IOS-XR devices.</p>

## Example Configuration: Provisioning an L3VPN Service

The following are examples of the configuration deployed to a Cisco ASR 9000 device with the following parameters:

- Creation of VRF and IP addresses (both IPv4 and IPv6) under the BDI (virtual) interface.
- Redistribution of OSPF protocol to the BGP protocol.

Example: Provisioning an L3VPN service on a Cisco ASR 9000 device's BVI enabled interface (sub-interface).

```
vrf vrfrbvibdi9k
vpn id aaaaaa:21
address-family ipv4 unicast
  import route-target
    6:55
address-family ipv6 unicast
  import route-target
    6:55
  export route-target
    6:55
interface GigabitEthernet0/0/0/17
  no shutdown
  exit
interface GigabitEthernet0/0/0/17.1
  encapsulation dot1q 1198
  shutdown
interface BVI 1
  vrf vrfrbvibdi9k
  ipv4 address 88.7.6.4 255.224.0.0
l2vpn
  bridge group BDI1
  bridge-domain 1
  routed interface BVI 1
  interface GigabitEthernet0/0/0/17.1
router bgp 140
  vrf vrfrbvibdi9k
  rd auto
  address-family ipv6 unicast
  address-family ipv4 unicast
  exit
  exit
  exit
```

Example: Using a BVI enabled interface for provisioning an L3VPN service with OSPF route distribution (using dual AS):

```
vrf definition VRF2-2VRF-2UNI-BDI
vpn id AAAAAA:2
rd 532533:2
address-family ipv4
  route-target import 6:5
  route-target export 6:5
address-family ipv6
  route-target export 6:5
interface GigabitEthernet0/0/0
  duplex full
  service instance 2 ethernet
  encapsulation dot1q 761
  bridge-domain 14
  shutdown
  exit
interface BDI14
  vrf forwarding VRF2-2VRF-2UNI-BDI
  ip address 5.44.3.7 255.255.0.0
router bgp 120
  address-family ipv4 vrf VRF2-2VRF-2UNI-BDI
  neighbor 55.4.3.2 remote-as 71
  neighbor 55.4.3.2 activate
```

```

redistribute rip metric 6
neighbor 55.4.3.2 local-as 387
address-family ipv6 vrf VRF2-2VRF-2UNI-BDI
neighbor c5::98 remote-as 50
neighbor c5::98 activate
redistribute ospf 65 match external metric 2
neighbor c5::98 local-as 324 no-prepend replace-as dual-as
exit
exit

```

## View L3VPN Service Details

Using Cisco EPN Manager , you can view the detailed information about an L3VPN service in the following ways:

- **Using the Circuit/VC 360 View:** The Circuit/VC 360 view provides detailed information available for a specific L3VPN created using Cisco EPN Manager . See [View Circuits/VCS](#). The different parameters associated with the L3VPN service are displayed in three different tabs: Summary, VRFs, Site Details, and PE-CE Routing.
- **Using the Network Topology and Service Details View:** The Network Topology window presents a graphical, topological map view of devices, the links between them, and the active alarms on the devices or links. It also enables you to visualize L3VPNs within the displayed topology map.
  - To view a complete list of L3VPNs and its details, see [View a Device Group's Circuits/VCS List in the Topology Window, on page 535](#). See, [Get Quick Information About a Circuit/VC: Circuit/VC 360 View](#).
  - To view the L3VPN service details for a specific device, see [View a Specific Device's Circuits/VCS](#)
- **Using the Alarms Table:** The Alarms Table in Cisco EPN Manager provides several ways to see, at a glance, if there are any problems with your L3VPN services. See [Check Circuits/VCS for Faults](#).

## Modify L3VPNs and VRFs

You can modify L3VPN services that are created and deployed using Cisco EPN Manager . While the full mesh prefix, QoS profiles, and RT values associated with the service can be modified, you cannot modify parameters such as the customer details, VPN name, and service MTU values associated with the service. To modify these parameters, delete the service, and re-create it with new values. You can also modify the VRFs associated with L3VPN services.

To modify L3VPN services and VRFs:

### Before you begin

To modify L3VPN services that are discovered and promoted using Cisco EPN Manager , you must ensure that the route distinguisher for the L3VPN service is specified in the format **rd device\_ip:number**. For example:

```

vrf definition vdvvgfr420
  rd 10.104.120.133:420
  vpn id 36B:420
  !
address-family...

```

If the route distinguisher is specified in any other format, you will not be able to edit the service.

- 
- Step 1** Navigate to **Maps > Network Topology**.
- Step 2** Click the **Circuits/VCs** tab, and select the L3VPN service that you want to modify.
- Step 3** Click the pencil (**Modify**) icon.
- Step 4** To modify the selected L3VPN, choose **Modify VPN** and click **Next**.  
The Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN.
- Step 5** To modify the VRFs associated with the selected L3VPN, choose **Modify VRF** and click **Next**.  
The Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN. Along with modifying existing VRF parameters, you can also associate new Route Target values to the VRF.  
While modifying VRFs, you cannot modify the QoS profiles associated with the UNIs, however, you can modify the QoS policies associated with the service endpoints.
- Note** You cannot modify the VRF name and device associated with the selected L3VPN.
- Step 6** Make the required changes and click **Submit** to preview the configuration that will be deployed to the device.
- Note** When you modify a VPN, you cannot change the VRFs associated with the VPN. To modify the VRFs, see [Add and Copy VRFs to an L3VPN Service, on page 482](#).
- Step 7** Review your changes and click **Deploy** to deploy your changes to the device.  
In case of a deploy failure on even a single device that is part of the service, the configuration is rolled back on all devices participating in the service.
- Step 8** To verify that your changes were saved, view the L3VPN service details. See [View L3VPN Service Details, on page 481](#).
- 

## Add and Copy VRFs to an L3VPN Service

Using Cisco EPN Manager you can create and associate new VRFs to existing L3VPN services. You can also copy the route target and other details from existing VRFs to create new VRFs for the L3VPN service.

To associate new VRFs with an L3VPN service:

- 
- Step 1** Navigate to **Maps > Network Topology**.
- Step 2** Click the **Circuits/VCs** tab and select the L3VPN service to which you want to associate new VRFs.  
You can also access the L3VPN Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.
- Step 3** Click the pencil (**Modify**) icon.  
The L3VPN Provisioning wizard is displayed.
- Step 4** Select **Add VRF** and click **Next**.
- Step 5** Click the + icon to add the new VRF details manually. To auto populate the VRF details, click the device on the map to select it. The device details and a new name for the VRF are automatically populated on the VRF's page.
- Step 6** You can copy VRF details from an existing VRF by clicking the **Copy From** drop-down list and selecting the required VRF.



Only those VRFs that are associated with the selected L3VPN are displayed along with the VRFs route target, and route redistribution details.

**Step 7** Otherwise, manually specify the details of the VRFs that you want to add to the selected VPN service. For more information about the different VRF parameters, see, [Create and Provision a New L3VPN Service](#).

**Step 8** Make any required changes such as adding endpoint and BGP neighbor details and click **Submit**.

**Step 9** Preview the configuration that is to be deployed to the device, make the required changes, and click **Deploy** to deploy the changes to the device.

To verify that your changes were deployed, view the selected L3VPN service's details. See [View L3VPN Service Details](#).

For more information on modifying and deleting L3VPN services, see [Delete an L3VPN Service Endpoint, on page 548](#) and [Modify L3VPNs and VRFs, on page 481](#).

---

## Provision Circuit Emulation Services

- [Summary of Cisco EPN Manager CEM Provisioning Support, on page 483](#)
- [Prerequisites for CEM Provisioning, on page 483](#)
- [Create and Provision a New CEM Service, on page 483](#)

### Summary of Cisco EPN Manager CEM Provisioning Support

Cisco EPN Manager supports the provisioning of Circuit Emulation (CEM) services. CEM provides a bridge between the traditional TDM network and the packet switched network (PSN). It encapsulates the TDM data into packets, provides appropriate header, and send the packets through PSN to the destination node. For more information, see [Supported Circuit Emulation Services, on page 425](#).

You can also assign a MPLS TE tunnel to a CEM service to allow the CEM service to traverse through the network. Use the **Preferred Path** drop-down list in the Provisioning Wizard to assign a MPLS TE tunnel for a CEM service. For more information, see [CEM Service Details References, on page 485](#).

### Prerequisites for CEM Provisioning

The following prerequisites must be met before you can provision a CEM service:

- IP/MPLS connectivity must be enabled on the originating and terminating endpoints in a CEM service.
- CEM configurations such as loopback interface and ACR groups must be configured on the devices that will be used in the CEM service. For more information, see [Configure Circuit Emulation , on page 275](#).
- Inventory collection status for the devices on which the CEM service will be provisioned must be *Completed*. To check this, go to **Inventory > Device Management > Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
- Optionally, customers can be created in the system so that you can associate a CEM service to a customer during the service creation and provisioning process. From the left sidebar, choose **Inventory > Other > Customers** to create and manage customers.

### Create and Provision a New CEM Service

The process of creating and provisioning a CEM service in Cisco EPN Manager involves:

- Specifying endpoints of the CEM service.
- Defining the attributes that influence how traffic that is delivered over the CEM service and through its endpoints will be treated.

### Before you begin

For information about the prerequisites that must be met before you can provision a CEM service, see [Prerequisites for CEM Provisioning, on page 483](#).

- 
- Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click **Device Groups**, and then select the location in which you want to create the CEM service.
- Step 3** Close the **Device Groups** popup window.
- Step 4** In the **Network Topology** window, click **Circuits/VCs**.
- Step 5** Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.
- You can also access the Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.
- Step 6** From the **Technology** drop-down list, choose **Circuit Emulation**.
- Step 7** From the **Service Type** drop-down list, choose the required CEM service type depending on the rate at which you want the circuit to transmit the data. For a list of CEM service types that Cisco EPN Manager supports, see [Supported Circuit Emulation Services, on page 425](#).
- Step 8** If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles, on page 509](#).
- Step 9** Click **Next** to go to the **Customer Service Details** page.
- Step 10** (Optional) Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then go to the Provisioning Wizard to start provisioning the CEM service.
- Step 11** Check the **Activate** check box to activate the interface associated with the service that you are provisioning.
- Step 12** Enter the service name and its description.
- Step 13** In the **Deployment Action** field, specify what you want to do when the CEM service creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.
- Step 14** Click **Next**, and then enter the A End and Z End configurations, and the transport settings for the CEM service. See [CEM Service Details References, on page 485](#) for descriptions of the fields and attributes.
- Step 15** If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, check the **Unmanaged Device** check box and provide information for the unmanaged device. See [Provision a Circuit/VC with an Unmanaged Endpoint, on page 511](#) for more information.
- Note** The **Unmanaged Device** check box is available only in the Z End Configurations page.
- Step 16** (Optional) If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the **Template Details** page. See [Extend a Circuit/VC Using Templates, on page 512](#) for more information.
- Step 17** When you have provided all the required information for the service, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.
-

The CEM service should be added to the list in the Circuits/VCs pane in the **Network Topology** window. To check the provisioning state, click on the *tei* icon next to the circuit/VC name to see the Circuit/VC 360 view.

## CEM Service Details References

The following table lists and describes the attributes that define the CEM service types.

**Table 37: Circuit Section Reference—CEM Service Types**

Attribute	Description
<b>A End and Z End Configurations</b>	
Device	Name of the source and destination devices in the CEM service.
<b>Working Path and Protecting Path</b>	
<b>Note</b>	The <b>Working Path and Protecting Path</b> are not available for X.21, C37.94, and EM-Voice service types.
Port Name or Interface Name	<p>Name of the interface on the source and destination devices in the CEM service. You can choose either the port name or the port group.</p> <p>When you choose the port name under the <b>Protecting Path</b> area, the unidirectional path switched ring (UPSR) protection mechanism is enabled.</p> <p>When you choose the port group under the <b>Protecting Path</b> area, the Automatic Protection Switching (APS) protection mechanism is enabled. For more information about how to configure protection groups, see <a href="#">Configure APS and UPSR Protection Groups, on page 279</a>.</p>
Higher Order Path	<p>When a SONET/SDH line is channelized, it is logically divided into smaller bandwidth channels called higher order paths (HOP) and lower order paths (LOP). HOP or synchronous transport signal (STS) path is used to transport TDM data of higher bandwidth. HOPs can also contain LOPs within it.</p> <p>Select the path and path mode available for the CEM service.</p>
Lower Order Path	LOPs or virtual tributary (VT) path is used to transport TDM data of lower bandwidth.
DS0 Time Slot	<p>Choose one or more time slots available in the DS0 group.</p> <p><b>Note</b> This field is available only if you select <b>DS0</b> in the <b>Service Type</b> field.</p>
<b>Clocking</b>	
<p>The nodes in a network may be at different clock rates. Differences in timing at nodes may cause the receiving node to either drop or reread information sent to it. Clocking is essential to synchronize all nodes to the same clock rate. For more information about clocking, see <a href="#">Configure Clocking for CEM, on page 281</a>.</p>	

Attribute	Description
Clock Source	<p>Enables to recover the clock rate from single source so that all nodes can be synchronized at the same clock rate. Values are:</p> <ul style="list-style-type: none"> <li>• Internal – Clock rate recovered from the host.</li> <li>• Line – Clock rate recovered from the SONET/SDH line.</li> <li>• Adaptive Clock Recovery – Clock rate is recovered based on the dejitter buffer fill level. Due to delay variations, the dejitter buffer fill levels keep varying continuously. The TDM service clock is recovered after filtering the variations. The accuracy of the recovered clock depends on the delay variations.</li> <li>• Differential Clock Recovery – Clock rate is recovered from a master clock using Sync-E. For more information about how to setup the master clock for your network, see <a href="#">Synchronize the Clock Using Sync-E, BITS, and PTP, on page 288</a>.</li> </ul>
Clock Rate	<p>Select the required clock rate in bits per second (bps). For example, if the clock rate is set to 64000, you can only send 64 kbps over the serial interface.</p> <p><b>Note</b> This field is available only for X.21 service type.</p>

### QoS

The list of profiles available for selection includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. Refer to [Create QoS Profiles, on page 510](#) for information on how to create QoS profiles.

Ingress QoS Profile	Select the ingress QoS policies that are configured on the A end and Z end devices.
---------------------	-------------------------------------------------------------------------------------

### Unmanaged Device Details

**Note** The below fields are available only for Z End Configurations.

Unmanaged Device	Check this check box to include a device that is not managed by Cisco EPN Manager and create partial service.
New Device	Check this check box to create a new unmanaged device.
Device	<p>Choose an unmanaged device from the drop-down list.</p> <p><b>Note</b> This field is available only when the <b>New Device</b> check box is unchecked.</p>
Device Name	<p>Enter a unique name for the new unmanaged device that you want to create.</p> <p><b>Note</b> This field is available only when the <b>New Device</b> check box is checked. If the <b>New Device</b> check box is unchecked, the name of the unmanaged device that you chose in the <b>Device</b> drop-down list is populated in this field.</p>

Attribute	Description
Device IP	<p>Enter the IP address of the new unmanaged device that you want to create.</p> <p><b>Note</b> This field is available only when the <b>New Device</b> check box is checked. If the <b>New Device</b> check box is unchecked, the IP address of the unmanaged device that you chose in the <b>Device</b> drop-down list is populated in this field.</p>
LDP IP	Enter a valid LDP IP for the unmanaged device.
VC ID	Enter a unique Virtual Circuit (VC) ID for the unmanaged device.
Time Slot	<p>Enter the time slot for the service. The valid range is 112.</p> <p><b>Note</b> This field is available only for C37.94 service type.</p>
Command Type	<p>Select the PCM encoding configuration for voice port. The values are A Law and U Law.</p> <p><b>Note</b> This field is available only for EM-Voice service type.</p>
Operation	<p>Select the number of wires used for voice transmission at this interface. The values are:</p> <ul style="list-style-type: none"> <li>• Wire 2—The audio path is full duplex with one pair of wires.</li> <li>• Wire 4—The audio path is full duplex with two pairs of wires.</li> </ul> <p><b>Note</b> This field is available only for EM-Voice service type.</p>
EM Signal	<p>Select the options of signaling type configuration. The values are:</p> <ul style="list-style-type: none"> <li>• Delay Dial—The originating end goes off-hook and waits for about 200 ms, then checks to see if the destination end is on-hook. If the destination end is on-hook, the originating end sends the dial digits. If the destination end is off-hook, the originating end waits till the destination end is on-hook, and then sends the dial digits.</li> <li>• Immediate Start—The originating end goes off-hook, waits for a finite period of time (for example, 200 ms), then sends the dial digits to the destination end.</li> <li>• Wink Start—The originating end goes off-hook, waits for a temporary off-hook pulse from the destination end (which is interpreted as an indication to proceed), then sends the dial digits.</li> </ul> <p><b>Note</b> This field is available only for EM-Voice service type.</p>
EM Type	<p>Select the type of E&amp;M interface to which the voice port is connecting. The values are Type 1, Type 2, Type 3, Type 5, and Type To.</p> <p><b>Note</b> This field is available only for EM-Voice service type.</p>

Attribute	Description
Impedence	<p>Select the impedance depending on the operation selected. If you selected the Operation as Wire 2, select the impedance as 600 R, Complex1, Complex2, or Complex3. If you selected the Operation as Wire 4, select the impedance as 600 R.</p> <p><b>Note</b> This field is available only for EM-Voice service type.</p>
<b>Transport Settings</b>	
Frame Type	<p>This field is display-only and is auto-populated based on the CEM service type that you chose when creating the CEM service. The values are CESoPSN, SAToP, and CEP.</p> <p>For T1 and T3 CEM service types, choose the frame type as SAToP or FRAMED_SATOP.</p>
Payload Size	<p>Number of bytes put into each IP packet. The valid range is 64 – 1312. The range will vary based on the device capability, level of support and the configured dejitter buffer size value.</p> <p><b>Note</b> For X.21 service type, the range will vary based on the clock rate.</p>
Dejitter Buffer Size	<p>Determines the ability of the emulated circuit to tolerate network jitter. The valid range is 1 - 32. The range will vary based on the device capability, level of support and the configured payload size value.</p> <p><b>Note</b> For X.21 service type, the range will vary based on the clock rate.</p>
Idle pattern	Idle pattern to transmit the data when the service goes down. The valid range is 0x00 - 0xFF.
Dummy Mode	Enables you to set a bit pattern for filling in for lost or corrupted frames. The values are last-frame and user-defined.
Dummy Pattern	<p>The bit pattern used for filling in for lost or corrupted frames. The valid range is 0x00 - 0xFF. The default is 0xFF.</p> <p><b>Note</b> This field is enabled only if you choose the Dummy Mode as user-defined.</p>
RTP Header Enabled	Check this check box to enable the Real-Time Transport Protocol (RTP) header for the CEM service.
RTP Compression Enabled	Check this check box to compress the IP header in a packet before the packet is transmitted. It reduces network overhead and speeds up the transmission of RTP.
<b>Pseudowire Settings</b>	
Preferred Path Type	Choose the Preferred Path Type as Bidirectional or Unidirectional.

Attribute	Description
Preferred Path	<p>Select the MPLS bidirectional TE tunnel through which you want the CEM service to pass through.</p> <p><b>Note</b> This field is available only if you selected <b>Bidirectional</b> as the Preferred Path Type.</p>
Preferred Path (A-Z)	<p>Select the required unidirectional tunnel through which you want the CEM service to travel from the A endpoint to the Z endpoint.</p> <p><b>Note</b> This field is available only if you selected <b>Unidirectional</b> as the Preferred Path Type.</p>
Preferred Path (Z-A)	<p>Select the required unidirectional tunnel through which you want the CEM service to travel from the Z endpoint to the A endpoint.</p> <p><b>Note</b> This field is available only if you selected <b>Unidirectional</b> as the Preferred Path Type.</p>
Allow Fallback to LDP	<p>Check this check box to ensure that the CEM service falls back to the default MPLS Label Distribution Protocol (LDP) when the selected preferred path goes down.</p> <p><b>Note</b> This check box is available only when you select a valid MPLS TE tunnel in the <b>Preferred Path</b> field.</p>
Send Control Word	<p>Check this check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.</p>

## Provision MPLS Traffic Engineering Services

- [Summary of Cisco EPN Manager MPLS TE Provisioning Support, on page 489](#)
- [MPLS TE Service Provisioning Features, on page 489](#)
- [Prerequisites for Provisioning an MPLS TE Service, on page 490](#)
- [Create and Provision an MPLS TE Tunnel, on page 490](#)
- [Create and Provision an MPLS Layer 3 Link, on page 498](#)

## Summary of Cisco EPN Manager MPLS TE Provisioning Support

Cisco EPN Manager supports the provisioning of MPLS Traffic Engineering services. MPLS TE enables an MPLS backbone to replicate and expand the TE capabilities of Layer 2 over Layer 3. MPLS TE uses Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP) across the backbone. For more information, see [Supported MPLS Traffic Engineering Services, on page 428](#).

## MPLS TE Service Provisioning Features

Cisco EPN Manager supports the following MPLS TE features:

- Support for constraint-based routing, and trunk admission control.
- Provision for path protection mechanism against link and node failures.
- Usage of Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP).
- Ability to advertise TE links using OSPF and ISIS.

**Note**

For the list of devices that support the provisioning of MPLS TE tunnel, see [Cisco Evolved Programmable Network Manager Supported Devices](#)

## Prerequisites for Provisioning an MPLS TE Service

The following prerequisites must be met before you can provision an MPLS TE service:

- OSPF or IS-IS must be configured on the devices that participate on the MPLS TE service.
- All links that will be used for MPLS TE service provisioning must be TE enabled.
- The TE enabled links must be operationally up.
- The tunnel's source and destination nodes must be reachable.
- MPLS reachability must be set up between the devices. MPLS core network configuration must be set up.
- Inventory collection status for the devices on which the MPLS TE service will be provisioned must be Completed. To check this, go to **Inventory > Device Management > Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
- Optionally, customers can be created in the system so that you can associate an MPLS TE service to a customer during the service creation and provisioning process. From the left sidebar, choose **Inventory > Other > Customers** to create and manage customers.

## Create and Provision an MPLS TE Tunnel

To provision an MPLS TE tunnel:

### Before you begin

For information about the prerequisites that must be met before you can provision an MPLS TE tunnel, see [Prerequisites for Provisioning an MPLS TE Service, on page 490](#)

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
  - Step 2** Click **Device Groups**, and then select the location in which you want to create the MPLS TE tunnel.
  - Step 3** Close the **Device Groups** popup window.
  - Step 4** In the **Network Topology** window, click **Circuits/VCs**.
  - Step 5** Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.



- Step 6** From the **Technology** drop-down list, choose **MPLS TE**. Cisco EPN Manager displays a list of relevant service types in a **Service Type** area.
- Step 7** In the **Service Type** area, choose **Unidirectional TE Tunnel** or **Bidirectional TE Tunnel**.
- Step 8** If you have defined profiles to set the attributes of the different services, choose the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles](#), on page 509.
- Step 9** Click **Next** to go to the **Customer Service Details** page.
- Step 10** (Optional) Select the customer for whom the service is being provisioned. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning wizard.
- Step 11** Enter the service name and its description, and then enter the service details. See [Field References for Service Details—MPLS TE Tunnel](#), on page 491.
- Note** If you do not provide a service name, Cisco EPN Manager assigns a service name in the following format:
- If the source and destination devices have a common tunnel ID, the service name is assigned in the <SourceDeviceName>\_<TunnelId>\_<DestinationDeviceName> format.
  - If the source and destination devices have unique tunnel IDs, the service name is assigned in the <SourceDeviceName>\_<ATunnelId>\_<ZTunnelId>\_<DestinationDeviceName> format.
- Step 12** Click **Next**, and then enter the tunnel creation parameters. See [Field References for Tunnel Creation—MPLS TE Tunnel](#), on page 492 for descriptions of the fields and attributes.
- Step 13** Click **Next**, and then enter the path constraint details. See [Field References for Path Constraint Details—MPLS TE Tunnel](#), on page 496 for descriptions of the fields and attributes.
- Step 14** Click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

---

The service should be added to the list in the Circuits/VCS pane in the **Network Topology** window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

## Field References for Service Details—MPLS TE Tunnel

The following table lists and describes the attributes that define the service details for creating a MPLS TE tunnel.

**Table 38: Service Details Section Reference—MPLS TE Tunnel**

Attribute	Description
Enable FRR	<p>Check this check box to enable the fast reroute feature that provides link and node protection for your MPLS TE tunnel.</p> <p><b>Note</b> This check box is available only when you create a unidirectional TE tunnel.</p>
Enable Auto Bandwidth	<p>Check this check box to automatically assign maximum and minimum bandwidth to the TE tunnel based on the traffic.</p> <p><b>Note</b> This check box is available only when you create a unidirectional TE tunnel.</p>

Attribute	Description
Wrap Protection	Check this check box to detect mid-link failure scenarios.  <b>Note</b> This check box is available only when you create a bidirectional TE tunnel.
Enable Fault OAM	Check this check box to enable the fault OAM protocols and messages that support the provisioning and maintenance of MPLS TE tunnels.  <b>Note</b> This check box is available only when you create a bidirectional TE tunnel.
Enable Autoroute	Check this check box to enable autoroute for the tunnel.
Enable LockDown	Check this check box if you do not want to reoptimize the working LSP.
Enable BFD Settings	Check this check box to enable the Bidirectional Forwarding Detection (BFD) protocol. BFD provides fast forwarding path failure detection time and a consistent failure detection method.
Protection Type	Choose one of the following protection mechanism for the TE tunnel: <ul style="list-style-type: none"> <li>• Working—The tunnel has only a working path.</li> <li>• Working+Protected—The tunnel has a working and a protected path, wherein if the working path fails, the traffic flow is automatically routed to the protected path without the links going down.</li> <li>• Working+Restore—The tunnel has a working and a restore path, wherein if the working path fails, the link goes down and then the traffic flow is routed to the restore path.</li> <li>• Working+Protected+Restore—The tunnel has a working, protected, and restore path, wherein, if the working path fails, the traffic flow is routed to the protected path. If the protected path also fails, the link goes down and then the traffic flow is routed to the restore path.</li> </ul>
Deployment Action	Choose one of the following options to specify what you want to do when the MPLS TE tunnel creation process is completed: <ul style="list-style-type: none"> <li>• Preview—Previews the configurations that will be deployed to the relevant devices before the actual deployment.</li> <li>• Deploy—Deploys the configurations immediately upon completion.</li> </ul>

## Field References for Tunnel Creation—MPLS TE Tunnel

The following table lists and describes the attributes that define the MPLS TE tunnel creation.

**Table 39: Tunnel Creation Section Reference—MPLS TE Tunnel**

Attribute	Description
<b>Create Tunnel</b>	
Source	Source or A endpoint of the tunnel.

Attribute	Description
Source routing Process	OSPF or ISIS routing process that is TE enabled and configured on the source endpoint selected. You can determine the router ID and loopback address configured on the source endpoint based on the OSPF or ISIS routing process.
Destination	Destination or Z endpoint of the tunnel.
Destination Routing Process	OSPF or ISIS routing process that is TE enabled and configured on the destination endpoint selected. You can determine the router ID and loopback address configured on the destination endpoint based on the OSPF or ISIS routing process.
<b>Tunnel Setting</b>	
Global ID	<p>The global ID assigned to both, source and destination endpoints. This ID must be the same to bind two unidirectional tunnels into a bidirectional TE tunnel. The default value is 0.</p> <p><b>Note</b> This attribute is available only when you create a bidirectional TE tunnel.</p>
Affinity Bits	The affinity bit determines the link attribute that the bidirectional TE tunnel will use when configuring the dynamic backup paths.
Affinity Mask	<p>The affinity mask determines which link attribute the router must check.</p> <p>You can use affinity bits and affinity mask to include or exclude link attributes when configuring the dynamic backup paths. If a bit in the mask is 0, the value of the associated link attribute for that bit is irrelevant. In this case, the link attribute is excluded when configuring the dynamic backup paths. If a bit in the mask is 1, the value of the associated link attribute must match the affinity of the tunnel for that bit. In this case, the link attribute is included when configuring the dynamic backup paths.</p>
Setup Priority	<p>Setup priority assigned to an LSP for the unidirectional or bidirectional TE tunnels. Based on this priority, the LSP can determine which existing tunnels or LSPs with low priority can be blocked.</p> <p>Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a setup priority of 0 can block any LSP with a setup priority between 1 and 7.</p> <p><b>Note</b> Setup priority cannot be higher than the hold priority.</p>
Hold Priority	<p>Hold priority assigned to an LSP for the unidirectional or bidirectional TE tunnels. Based on this priority, the LSP can determine whether it must be blocked by another signaling LSP with a high setup priority.</p> <p>Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a hold priority of 0 cannot be blocked by another LSP.</p>

Attribute	Description
Bandwidth Pool Type	<p>Bandwidth pool used to manage the reservable bandwidth on each link for constraint-based routing (CBR) in MPLS TE. Values are:</p> <ul style="list-style-type: none"> <li>• Global – Regular TE tunnel bandwidth.</li> <li>• Subpool – A portion of the global pool. The subpool bandwidth is not reserved from the global pool if it is not in use. Subpool tunnels require a higher priority than global pool tunnels.</li> </ul> <p><b>Note</b> This field is available only when you uncheck the <b>Enable Auto Bandwidth</b> check box.</p>
Bandwidth	<p>Bandwidth for the bidirectional TE tunnel. The value must be specified in the units of Kbps.</p> <p>For example, if you want to assign a bandwidth of 1000000 Kbps for the tunnel, enter the value as 1000000 Gbps.</p> <p><b>Note</b> This field is available only when you uncheck the <b>Enable Auto Bandwidth</b> check box.</p>
Auto Bandwidth Max	<p>Cisco EPN Manager automatically assigns the maximum bandwidth for the unidirectional TE tunnel based on the traffic. However, you can change the bandwidth, if required.</p> <p><b>Note</b> This field is available only when you check the <b>Enable Auto Bandwidth</b> check box in the <b>Customer Service Detail</b> screen.</p>
Auto Bandwidth Min	<p>Cisco EPN Manager automatically assigns the minimum bandwidth for the unidirectional TE tunnel based on the traffic. However, you can change the bandwidth, if required.</p> <p><b>Note</b> This field is available only when you check the <b>Enable Auto Bandwidth</b> check box in the <b>Customer Service Detail</b> screen.</p>
Bandwidth Change Frequency (Sec)	<p>Enter the bandwidth change frequency in seconds. The valid range is between 3600 to 604800.</p> <p><b>Note</b> This field is available only when you check the <b>Enable Auto Bandwidth</b> check box in the <b>Customer Service Detail</b> page when you create unidirectional tunnels.</p>

Attribute	Description
Adjustment Threshold	<p>Enter the bandwidth adjustment threshold in percentage to trigger an adjustment if the largest sample percentage is higher or lower than the current tunnel bandwidth. . Adjustment threshold is the percentage of the current tunnel bandwidth and an absolute (minimum) bandwidth. Both the thresholds must be fulfilled for the automatic bandwidth to resignal the tunnel. The tunnel bandwidth is adjusted only if the difference between the largest sample output rate and the current tunnel bandwidth is larger than the adjustment thresholds.</p> <p>The valid range for the unidirectional tunnels that connect the Cisco IOS-XR devices is 1 to 100 and the range for the unidirectional tunnels that connect the Cisco IOS-XE devices is 1 to 99.</p> <p><b>Note</b> This field is available only when you check the <b>Enable Auto Bandwidth</b> check box in the <b>Customer Service Detail</b> page when you create unidirectional tunnels.</p>
Overflow Threshold	<p>Enter the overflow threshold in percentage to trigger the overflow detection. It is the percentage of the actual signalled tunnel bandwidth. When the difference between the measured bandwidth and the actual bandwidth is larger than the overflow threshold percentage for the N consecutive times (defined as the overflow limit), an overflow detection is triggered.</p> <p>The valid range for the unidirectional tunnels that connect the Cisco IOS-XR devices is 1 to 100 and the range for the unidirectional tunnels that connect the Cisco IOS-XE devices is 1 to 99.</p> <p><b>Note</b> This field is available only when you check the <b>Enable Auto Bandwidth</b> check box in the <b>Customer Service Detail</b> page when you create unidirectional tunnels.</p>
Overflow Limit	<p>Enter the number of consecutive collection periods during which the difference between the measured bandwidth and the actual bandwidth of a tunnel can exceed the overflow threshold defined for the tunnel.</p> <p>The valid range is 1 to 10.</p> <p><b>Note</b> This field is available only when you check the <b>Enable Auto Bandwidth</b> check box in the <b>Customer Service Detail</b> page when you create unidirectional tunnels.</p>
Collect Bandwidth	<p>Check this check box to collect the bandwidth information for the unidirectional tunnel.</p> <p><b>Note</b> This field is available only when you check the <b>Enable Auto Bandwidth</b> check box in the <b>Customer Service Detail</b> page when you create unidirectional tunnels.</p>
<b>BFD Settings</b>	

Attribute	Description
Min Interval	BFD uses intervals and multipliers to specify the periods at which control and echo packets are sent in asynchronous mode and their corresponding failure detection. A failure detection timer is started based on $(I \times M)$ , where $I$ is the minimum interval, and $M$ is the multiplier.
Multiplier	
	<b>Note</b> These fields are available only when you check the <b>Enable BFD Settings</b> check box.

## Field References for Path Constraint Details—MPLS TE Tunnel

The following table lists and describes the attributes that define the path constraint details for creating a MPLS TE tunnel.

**Table 40: Path Constraint Details Section Reference—MPLS TE Tunnel**

Attribute	Description
Path Type	Choose the required path for the TE tunnel. The values are <b>Working</b> , <b>Protected</b> , and <b>Restore</b> .
<b>Working Path, Protection Path, and Restore Path</b> Based on the value you choose in the <b>Path Type</b> field, the respective field group is available.	
Type	Choose the type of working path or protected path for the tunnel. Values are <b>Dynamic</b> and <b>Explicit</b> .
New	Check this check box to create a new explicit working, protected, or restore path for the tunnel.  <b>Note</b> All the below fields are available only when you select <b>Explicit</b> in the <b>Type</b> field.
Select Existing Path	Choose an existing explicit working, protected, or restore path for the tunnel.  <b>Note</b> This field is available only when you uncheck the <b>New</b> check box.
Path Name	Enter a name for the explicit path that you are creating. In the <b>Working Path</b> , <b>Protection Path</b> , or <b>Restore Path</b> table, click the '+' button to add a new row to the table, and then select a MPLS-enabled device, an explicit path controller as the interface for the device, and a path constraint type.  In the path table, you can select any MPLS-enabled device except the source and destinations devices. Cisco EPN Manager supports only strict path constraint type.  <b>Note</b> This field is available only when you check the <b>New</b> check box.

Attribute	Description
<b>Working Path LSP Attribute List, Protection Path LSP Attribute List, and Restore Path LSP Attribute List</b>  Based on the value you choose in the <b>Path Type</b> field, the respective field group is available.  The LSP attributes that you define here are associated with the path option you selected in the <b>Path Type</b> field and these attributes are applicable for source and destination devices.  <b>Note</b> The values that are defined for a specific path option will override the values specified at the interface tunnel level. For example, if you have defined the LSP attributes for the working path, these values will override the values that you defined in the <b>Tunnel Settings</b> section at the interface tunnel level, which is common for all the path options.	
New LSP Attribute List	Check this check box to create a new LSP attribute list for the selected path type.
Existing LSP Attribute List	Choose an existing LSP attribute list for the selected path type.  <b>Note</b> This field is available only when you uncheck the <b>New LSP Attribute List</b> check box.
LSP Attribute List Name	Enter a name for the LSP attribute list that you are creating.  <b>Note</b> All the below fields including this field are available only when you check the <b>New LSP Attribute List</b> check box.
LSP Affinity Bits	Enter the LSP affinity bit that determines the link attribute that the bidirectional TE tunnel will use when configuring the backup paths (working, protected, or restore).
LSP Affinity Mask	Enter the LSP affinity mask that determines which link attribute the router must check when configuring the backup paths.
LSP Setup Priority	Enter the setup priority assigned to an LSP for the chosen path type. Based on this priority, the LSP can determine which existing tunnels or LSPs with low priority can be blocked.  Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a setup priority of 0 can block any LSP with a setup priority between 1 and 7.  <b>Note</b> LSP setup priority cannot be higher than the LSP hold priority.  <b>Note</b> For Cisco IOS-XR devices, the <b>LSP Setup Priority</b> and <b>LSP Hold Priority</b> fields are not applicable.

Attribute	Description
LSP Hold Priority	<p>Enter the hold priority assigned to an LSP for the chosen path type. Based on this priority, the LSP can determine whether it must be blocked by another signaling LSP with a high setup priority.</p> <p>Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a hold priority of 0 cannot be blocked by another LSP.</p> <p><b>Note</b> For Cisco IOS devices, if you do not specify an LSP hold priority, Cisco EPN Manager takes the value specified in the <b>LSP Setup Priority</b> field.</p> <p><b>Note</b> For Cisco IOS-XR devices, the <b>LSP Setup Priority</b> and <b>LSP Hold Priority</b> fields are not applicable.</p>
LSP Record Route	Check the check box to record the route used by the LSP.

## Create and Provision an MPLS Layer 3 Link

To provision an MPLS Layer 3 Link:


### Before you begin

For information about the prerequisites that must be met before you can provision an MPLS Layer 3 Link, see [Prerequisites for Provisioning an MPLS TE Service, on page 490](#).

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**
- Step 2** Click **Device Groups**, and then select the location in which you want to create the MPLS Layer 3 Link.
- Step 3** Close the **Device Groups** popup window.
- Step 4** In the **Network Topology** window, click **Circuits/VCs**.
- Step 5** Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.
- Step 6** From the **Technology** drop-down list, choose **MPLS TE**. Cisco EPN Manager displays a list of relevant service types in the **Service Type** area.
- Step 7** In the **Service Type** area, choose **Layer 3 Link**.
- Step 8** If you have defined profiles to set the attributes of the different services, choose the required profile from the **Select Profile** drop-down list. See [Create Circuit/VC Profiles, on page 509](#).
- Step 9** Click **Next** to go to the **Link Settings** page.
- Step 10** Enter a name and description for the layer 3 link.
- Step 11** Choose the **A End Device**, **A End Interface**, **Z End Device**, and **Z End Interface** fields using one of the following ways:
- Click a link on the map to automatically populate the **A End Device**, **A End Interface**, **Z End Device**, and **Z End Interface** fields.
  - Click a device node on the map to automatically populate the **A End Device** field. If the A End Device is connected to only one device, the **Z End Device** field is populated automatically. If the **A End Device** is connected to more than one device, you must choose the **Z End Device** manually.



- Step 12** Enter the IP address and mask for the A End and Z End devices.
- Step 13** Choose an L2 Discovery Protocol from the following options:
- **NONE**—No L2 discovery protocol to be enabled for the layer 3 link.
  - **CDP**—Cisco Discovery Protocol to be enabled for the layer 3 link to facilitate communication between Cisco devices connected to the network.
  - **LLDP**—Link Layer Discovery Protocol to be enabled for the layer 3 link to support non-Cisco devices and to allow for interoperability between other devices that supports the IEEE 802.1AB LLDP.
  - **ALL**—Both, CDP and LLDP to be enabled for the layer 3 link.
- Step 14** Choose the required routing protocol for the layer 3 link. The values are BGP, ISIS, and OSPF. For information about how to configure the routing protocols, see [Configure Routing Protocols and Security, on page 352](#)
- Step 15** (Optional) Enter a Link VLAN ID for the layer 3 link.
- Step 16** (Optional) Check the **Enable MPLS TE** check box to support MPLS TE on the layer 3 link that you are provisioning.
- Note** This check box is available only when you choose OSPF or ISIS as your routing protocol.
- Step 17** Click **Next**, and then enter the A End and Z End details. See [Field References for A End Details and Z End Details in MPLS Layer 3 Link, on page 499](#) for descriptions of the fields and attributes.
- Step 18** In the **Deployment Action** field, specify what you want to do when the MPLS layer 3 link creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.
- Step 19** Click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The service should be added to the list in the **Circuits/VCs** tab in the Network **Topology** window. To check the provisioning state, click the  icon next to the circuit/VC name to see the Circuit/VC 360 view.

## Field References for A End Details and Z End Details in MPLS Layer 3 Link

The following table lists and describes the attributes that define the MPLS Layer 3 Link.

**Table 41: Field References for A End and Z End Details—MPLS Layer 3 Link**

Attribute	Description	Available when the routing protocol is:
Same as A End	Check this check box if you want to have the same OSPF and MPLS-TE configurations for both A end and Z end devices.  <b>Note</b> This check box is available only in the Z End Details page of the Provisioning Wizard.	BGP, ISIS, and OSPF
BGP AS Number	Choose the unique BGP autonomous system number assigned for your network.	BGP
Route Policy	Choose the routing policy to control which routes the BGP stores in and retrieves from the routing table.	BGP

Attribute	Description	Available when the routing protocol is:
Route Reflector Client	Check this check box to configure the BGP neighbor as the route reflector client for the local route reflector to advertise the available routes.	BGP
Use AIGP	Check this check box to use the Accumulated Interior Gateway Protocol (AIGP) metric attribute for the layer 3 link. The AIGP is the BGP attribute that carries the accumulated end-to-end metrics for the paths in the network.	BGP
Update Source	Choose the required source interface.  <b>Note</b> This field is available only when the <b>Use AIGP</b> check box is unchecked.	BGP
ISIS Process ID	Choose an ISIS routing process ID that is available to both A end and Z end devices. For information about how to configure an ISIS process, see <a href="#">Configure an IS-IS, on page 356</a> .	ISIS
Network	The network ID is automatically populated based on the ISIS process ID selected.	ISIS
Circuit Type	Choose the type of adjacency required for the layer 3 link from the following options: <ul style="list-style-type: none"> <li>• NONE—No adjacency is established.</li> <li>• Level-1—Establishes a level 1 adjacency if there is at least one area address in common between the selected device and its neighbors.</li> <li>• Level-2-only—Establishes a level 2 adjacency on the circuit. If the neighboring device is a level 1 only device, no adjacency will be established.</li> <li>• Level-1-2—Establishes a level 1 and 2 adjacency if the neighbor is also configured as a level 1-2 device and there is at least one area in common. If there is no area in common, a level 2 adjacency is established.</li> </ul>	ISIS
Level 1 Metric	Enter the metric that must be used in the SPF calculation for Level 1 (intra-area) routing.  <b>Note</b> This field is available only when you choose the <b>Circuit Type</b> as <b>Level-1</b> or <b>Level-1-2</b> .	ISIS

Attribute	Description	Available when the routing protocol is:
Level 2 Metric	<p>Enter the metric that must be used in the SPF calculation for Level 2 (inter-area) routing.</p> <p><b>Note</b> This field is available only when you choose the <b>Circuit Type</b> as <b>Level-2</b> or <b>Level-1-2</b>.</p>	ISIS
OSPF Process ID	<p>Choose an OSPF routing process ID. For information about how to configure an OSPF process, see <a href="#">Configure OSPF, on page 358</a>.</p> <p><b>Note</b> You cannot modify the OSPF routing process for the Z end device.</p>	OSPF
OSPF Area	Enter the area in which you want to deploy the OSPF routing process.	OSPF
Metric	Enter the routing metric used by the OSPF routing process.	OSPF
BFD Template	Choose a BFD template for the layer 3 link. A BFD template defines the set of configurable parameters used by a BFD session. These include the transmit and receive timers used for BFD control and echo packets, the transmit timer interval used when the session is providing a CV function, the multiplier value, and the echo-receive interval.	BGP, ISIS, and OSPF
BFD Min Interval	<p>Enter the minimum control packet interval for BFD sessions for the corresponding BFD configuration scope.</p> <p><b>Note</b> This field is available only if you have not chosen the <b>BFD Template</b>.</p>	BGP, ISIS, and OSPF
BFD Multiplier	<p>Enter the BFD multiplier. This value along with the BFD minimum interval is used to determine the intervals and failure detection times for both control and echo packets in asynchronous mode on bundle member links.</p> <p><b>Note</b> This field is available only if you have not chosen the <b>BFD Template</b>.</p>	BGP, ISIS, and OSPF
BFD Fast Detect	<p>Check this check box to quickly detect failures in the path between adjacent forwarding engines.</p> <p>ISIS and OSPF</p>	

Attribute	Description	Available when the routing protocol is:
Authentication Mode	Choose the required authentication mode used to send and receive ISIS packets.  <b>Note</b> The authentication fields are available only when you select Cisco IOS and Cisco IOS XE devices.	ISIS
Authentication Key Chain	Choose the authentication key chain. This enables authentication for routing protocols and identifies a group of authentication keys.	ISIS
Authentication for Send Only	Check this check box to perform authentication only for ISIS packets that are being sent.	ISIS
Password Type	Choose the password type as <b>Encrypted</b> or <b>Plain Text</b> .	BGP
Password	Type the desired password. Password is required to establish connection between two peers.	BGP
<b>MPLS-TE</b>		
Loopback Interface	Choose a loopback interface address for the layer 3 link. For information about how to configure a loopback interface, see Configure Loopback Interfaces.	ISIS and OSPF
TE Metric	Enter the MPLS TE tunnel metric with mode absolute.	ISIS and OSPF
TE Attributes	Enter the MPLS TE Link attribute to be compared with a tunnel's affinity bits during path selection.	ISIS and OSPF
Is Percentage	Check this check box to assign the bandwidth in percentage for the layer 3 link.	ISIS and OSPF
Global Bandwidth	Enter the regular TE tunnel bandwidth that will be reserved for the layer 3 link for CBR.  For example, if you want to assign 10% as the global bandwidth for the layer 3 link, select the <b>Is Percentage</b> check box and enter the value 10 in the <b>Global Bandwidth</b> field. Whereas, if you want to assign 50 Kbps as the global bandwidth, uncheck the <b>Is Percentage</b> check box, choose Kbps from the <b>Bandwidth Unit</b> drop-down list, and then enter the value 50 in the <b>Global Bandwidth</b> field.	ISIS and OSPF

Attribute	Description	Available when the routing protocol is:
Subpool Bandwidth	Enter the subpool bandwidth that is reserved from the global pool bandwidth.  For example, if you want to assign 10% as the subpool bandwidth for the layer 3 link, select the <b>Is Percentage</b> check box and enter the value 10 in the <b>Subpool Bandwidth</b> field. Whereas, if you want to assign 50 Kbps as the subpool bandwidth, uncheck the <b>Is Percentage</b> check box, choose Kbps from the <b>Bandwidth Unit</b> drop-down list, and then enter the value 50 in the <b>Subpool Bandwidth</b> field.	ISIS and OSPF
<b>QoS</b>		
Ingress Policy	Select the ingress QoS policies that are configured on the A end and Z end devices.	BGP, ISIS, and OSPF
Egress Policy	Select the egress QoS policies that are configured on the A end and Z end devices.	BGP, ISIS, and OSPF
<b>Additional Settings</b>		
Enable MPLS	Check this check box to support MPLS on the layer 3 link that you are provisioning.	BGP
Enable SyncE	Check this check box to enable Synchronous Ethernet at the interface level for the layer 3 link.	BGP, ISIS, and OSPF

## Provision Serial Services

- [Prerequisites for Serial Circuits/VCs Provisioning, on page 503](#)
- [Create and Provision a New Serial Circuit/VC, on page 504](#)
- [Create and Provision a New Raw Socket Circuit/VC, on page 507](#)

## Prerequisites for Serial Circuits/VCs Provisioning

Following are the prerequisites to provision a serial circuit/VC:

- Communication between devices must be set up before you can provision a serial circuit/VC.
- Inventory collection status for the devices on which the Serial circuits/VCs will be provisioned must be "Completed". To check this, go to **Inventory > Device Management > Network Devices**, and look at the status in the Last Inventory Collection Status column.
- Optionally, customers must be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. From the left sidebar, choose **Inventory > Other > Customers** to create and manage customers.

## Create and Provision a New Serial Circuit/VC

To create a new serial circuit/VC:

### Before you begin

For information about the prerequisites that must be met before you can provision a serial circuit/VC, see [Prerequisites for Serial Circuits/VCs Provisioning, on page 503](#).

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.  
The network topology window opens.
- Step 2** From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.
- Step 3** Click the **Circuits/VCs** tab.
- Step 4** From the **Circuits/VCs** pane toolbar, click the + (**Create**) icon.  
The Provisioning Wizard opens in a new pane to the right of the map.
- Step 5** Select **Serial** in the Technology drop-down list.
- Step 6** In the Service Type list, select the type of serial service you want to create. For information about the serial service types that Cisco EPN Manager supports, see [Supported Serial Services, on page 429](#).
- Step 7** If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See [Create Circuit/VC Profiles, on page 509](#).
- Step 8** Click **Next** to go to the Service Details page.
- Step 9** Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.
- Step 10** Enter the service name and description.
- Step 11** In the Deployment Action field, specify what you want to do when the circuit/VC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.
- Step 12** Click Next to go to the page in which you configure the endpoints. See [Serial Service Details Reference, on page 505](#).
- Step 13** If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, provide information for the unmanaged device. See [Provision a Circuit/VC with an Unmanaged Endpoint, on page 511](#).
- Step 14** Click Next to go to the Line Settings and Pseudowire Settings page. See [Serial Service Details Reference, on page 505](#).
- Step 15** Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the circuit/VC, do so in the Template Details page. See [Extend a Circuit/VC Using Templates, on page 512](#) for more information.
- Step 16** When you have provided all the required information for the circuit/VC, click Submit. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.
- 

The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window.

## Serial Service Details Reference

The following table lists and describes the attributes that define the serial service type.

**Table 42: Circuit Section Reference—Serial Service Type**

Attribute	Description
<b>A Endpoint and Z Endpoint Configurations</b>	
Device Name	Name of the source and destination devices in the serial service.
Port Name and Description	Name and description of the interface on the source and destination devices in the serial service.
<b>QoS</b> The list of profiles available for selection includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles. Refer to <a href="#">Create QoS Profiles, on page 510</a> for information on how to create QoS profiles.	
Ingress QoS Profile	Select the ingress QoS policies that are configured on the A end and Z end devices.
Egress QoS Profile	Select the egress QoS policies that are configured on the A end and Z end devices.
<b>Unmanaged Device Details</b>	
<b>Note</b> The below fields are available only for Z Endpoint Configurations.	
Unmanaged Device	Check this check box to include a device that is not managed by Cisco EPN Manager and create partial service.
New Device	Check this check box to create a new unmanaged device.
Device Name	Enter a unique name for the new unmanaged device that you want to create. <b>Note</b> This field is available as a drop-down list if you have unchecked the <b>New Device</b> check box. You can choose an unmanaged device as your Z endpoint.
Device IP	Enter the IP address of the new unmanaged device that you want to create. <b>Note</b> This field is available only when the <b>New Device</b> check box is checked. If the <b>New Device</b> check box is unchecked, the IP address of the unmanaged device that you chose in the <b>Device</b> drop-down list is populated in this field.
LDP IP	Enter a valid LDP IP for the unmanaged device.
VC ID	Enter a unique Virtual Circuit (VC) ID for the unmanaged device.
<b>Line Settings</b>	
Speed	The speed of the serial link in kilo bits per second.
Data Bits	The measurement of actual data per packet that is transmitted through the serial circuit/VC. The values are 5, 6, 7, and 8.

Attribute	Description
Stop Bits	<p>Indicates the end of communication for a single packet. The values are 1, 1.5, and 2 bits.</p> <p>Since the data is clocked across the lines and each device has its own clock, it is possible for the two devices to become slightly out of sync. Therefore, the stop bits not only indicate the end of transmission but also provides the network with some lenience to synchronize the different clocks. The more bits that are used for stop bits, the greater the lenience in synchronizing the different clocks, but slower the data transmission rate.</p>
Flow Control In and Flow Control Out	Manages the rate of data transmitted between two devices when the source device transmits data at a faster rate than the destination device can receive it. It provides a mechanism for the source device to control the transmission speed, so that the destination device is not overwhelmed with data that is transmitted. The values are None, Hardware, and Software.
Flow Control Lock	Enables or disables the flow control mechanism for the serial circuit/VC. The values are True and False.
Parity	<p>Used to check errors in serial communication. The values are:</p> <ul style="list-style-type: none"> <li>• None—No parity defined for the circuit/VC.</li> <li>• Even— The serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an even number of logic high bits. For example, if the data was 011, then for even parity, the parity bit would be 0 to keep the number of logic high bits even.</li> <li>• Odd— The serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an odd number of logic high bits. For example, if the data was 011, then for odd parity, the parity bit would be 1, resulting in 3 logic high bits.</li> <li>• Mark— Sets the parity bit high. This allows the receiving device to know the state of a bit which enables the device to determine if noise is corrupting the data or if the transmitting and receiving devices' clocks are out of sync.</li> <li>• Space—Sets the parity bit low. This allows the receiving device to know the state of a bit which enables the device to determine if noise is corrupting the data or if the transmitting and receiving devices' clocks are out of sync.</li> </ul>
<b>Pseudowire Settings</b>	
Preferred Path Type	Choose the Preferred Path Type as Bidirectional or Unidirectional.
Preferred Path	<p>Select the MPLS bidirectional TE tunnel through which you want the serial service to pass through.</p> <p><b>Note</b> This field is available only if you selected <b>Bidirectional</b> as the Preferred Path Type.</p>



Attribute	Description
Preferred Path (A-Z)	<p>Select the required unidirectional tunnel through which you want the serial service to travel from the A endpoint to the Z endpoint.</p> <p><b>Note</b> This field is available only if you selected <b>Unidirectional</b> as the Preferred Path Type.</p>
Preferred Path (Z-A)	<p>Select the required unidirectional tunnel through which you want the serial service to travel from the Z endpoint to the A endpoint.</p> <p><b>Note</b> This field is available only if you selected <b>Unidirectional</b> as the Preferred Path Type.</p>
Send Control Word	Check this check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.

## Create and Provision a New Raw Socket Circuit/VC

To create a new Raw Socket circuit/VC:

### Before you begin

For information about the prerequisites that must be met before you can provision a Raw Socket circuit/VC, see [Prerequisites for Serial Circuits/VCs Provisioning, on page 503](#).

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.  
The network topology window opens.
- Step 2** From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.
- Step 3** Click the **Circuits/VCs** tab.
- Step 4** From the **Circuits/VCs** pane toolbar, click the + (**Create**) icon.  
The Provisioning Wizard opens in a new pane to the right of the map.
- Step 5** Select **Serial** in the Technology drop-down list.
- Step 6** In the Service Type list, select **Raw Socket**. For information about the Raw Socket circuits/VCs, see [Supported Serial Services, on page 429](#).
- Step 7** If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See [Create Circuit/VC Profiles , on page 509](#).
- Step 8** Click **Next** to go to the Customer Service Details page.
- Step 9** Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory > Other > Customer** to create the customer in the system, and then restart the Provisioning Wizard.
- Step 10** Enter the service name and description.
- Step 11** In the Deployment Action field, specify what you want to do when the circuit/VC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

- Step 12** Click **Next** to go to the Server Side Configuration page. See [Raw Socket Service Details Reference, on page 508](#) for descriptions of the fields and attributes.
- Step 13** Click **Next** to go to the Client Side Configuration page. Click the '+' icon in the Raw Socket Client table to add a new row for client side configuration. See [Raw Socket Service Details Reference, on page 508](#) for descriptions of the fields and attributes.
- Step 14** Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the circuit/VC, do so in the Template Details page. See [Extend a Circuit/VC Using Templates, on page 512](#) for more information.
- Step 15** When you have provided all the required information for the circuit/VC, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

---

The circuit/VC should be added to the list in the Circuits/VCS pane in the Network Topology window.

## Raw Socket Service Details Reference

The following table lists and describes the attributes that define the Raw Socket service type.

**Table 43: Raw Socket Service Type—Server Side and Client Side Configurations**

Attribute	Description
<b>Server Settings and Client Settings</b>	
Device Name	Name of the devices that act as a server and client in the Raw Socket service.
Port Name	Name of the interface on the server and client devices in the Raw Socket service.
Server Address and Server Port	The IP address and the port number of the server.
Client Address and Client Port	The IP address and the port number of the client.
Connection Idle Timeout	TCP session timeout setting for the Raw Socket service. If no data is transferred between the client and server over this interval, then the TCP session closes. The client then automatically attempts to reestablish the TCP session with the server.
VRF	Virtual Routing and Forwarding (VRF) interface through which the server and client are connected to transport the data.  <b>Note</b> Ensure that the VRF definition is common for both server and client.
<b>Packetization Settings</b>	
Packet Length	The packet length that triggers the routing device (either a server or a client) to transmit the serial data to the peer. When the device collects the specified bytes of data in its buffer, it packetizes the accumulated data and forwards it to the Raw Socket peer.

Attribute	Description
Packet Timer	Specifies the amount of time in milliseconds, the device (either server or client) waits to receive the next character in a stream. If a character is not received by the time the packet timer expires, the data the device has accumulated in its buffer is packetized and forwarded to the Raw Socket peer.
Special Char	A character that triggers the device (either server or client) to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the specified special character is received, the device packetizes the accumulated data and sends it to the Raw Socket peer.

## Create Circuit/VC Profiles

Profiles contain sets of attributes specific to the different types of circuits/VCs. Once a profile is created, it will be available to all users for selection during circuit/VC creation. When a profile is selected, the Provisioning Wizard is populated with the profile attributes. Users only have to define the endpoints of the service and, if necessary, make small changes before provisioning the circuit/VC.

The types of profiles you can create mirror the types of circuits/VCs that can be provisioned.

Each profile is given a unique name, so you can create multiple profiles per circuit/VC type, depending on your needs.

To create a profile:

- 
- Step 1** Choose **Inventory > Other > Profiles** in the left navigation pane. The **Profiles** window opens, showing a table of existing profiles (if any). You can select a profile in the table to edit or delete it.
- Step 2** Click **Create Profile**.
- Step 3** In the Create Profile wizard, provide a unique name for the profile and enter a description.
- Step 4** Select **Carrier Ethernet** or **Optical** or **L3VPN** from the **Technology** list. The relevant service types for the selected technology are displayed.
- Step 5** Select the required service type.
- For L3VPN services, choose **Unicast** to create a profile that helps pre-populate values for most L3VPN service creation fields. And choose **IPSLA Operations** to create a profile with IP SLA specific options for the L3VPN service.
- Step 6** Click **Next** to go to the attribute definition pages and define the attributes for the selected service type. The attributes in the profile are the same as the attributes in the Provisioning Wizard and they are described in the reference sections, as follows:
- Information on Ethernet VCs attributes is provided in these topics:
- For attributes relating to the service itself, see [Service Details Reference, on page 441](#)
  - For attributes specific to the UNI, see [New UNI Details Reference, on page 442](#)
  - For attributes relating to the UNI as it operates within the service, see [UNI Service Details Reference, on page 443](#).
  - For QoS Profile attributes, see [Create QoS Profiles, on page 510](#)
  - For UNI attributes, see [Configure a Device and Interface To Be a UNI, on page 445](#)
  - For ENNI attributes, see [Configure a Device and Interface To Be an ENNI, on page 446](#)

Information on OCH and OTN attributes is provided in [Circuit Section Reference for OCH Circuit Types, on page 450](#) and [Circuit Section Reference for OTN Circuit Types, on page 461](#).

Information on L3VPN attributes is provided in [Create and Provision a New L3VPN Service, on page 471](#) and [View L3VPN Service Details, on page 481](#).

**Step 7** Click **Create Profile** when you have defined the attributes. The profile will be added to the table in the Profiles window.

## Create QoS Profiles

You can create a library of QoS profiles that will be available for selection when creating and provisioning EVCs. The selected QoS profile determines the bandwidth profile for traffic of various classes on the UNI or the EVC level, and defines how the classified traffic is treated.

The QoS profile can define up to four levels of bandwidth profile: Extra High, High, Medium, and Low. For each bandwidth profile, you specify the matching criteria that must be met for the traffic to be classified as belonging to that bandwidth profile.

To create a QoS profile:

- 
- Step 1** Follow the instructions in [Create and Provision a New Carrier Ethernet EVC, on page 437](#) to access the Provisioning Wizard.
- Step 2** Select **Carrier Ethernet** from the Technology drop-down list.
- Step 3** Select **QoS Profile** from the Service Types drop-down list.
- Step 4** Click **Next** to go to the QoS Profile definition page.
- Step 5** Provide the QoS profile with a unique name and description.
- Step 6** Check the required check boxes to define where the QoS profile will be available for selection (i.e., it will appear in the drop-down list of QoS profiles):
- Applicable for Interfaces—The QoS profile will be available for selection when provisioning UNIs or ENNs.
  - Applicable for Virtual Services—The QoS profile will be available for selection as a UNI service attribute when creating VLAN-based services, such as EVPL, EV-LAN, and so on.
  - Applicable for Private Services—The QoS profile will only be available for selection as a UNI service attribute when creating private VCs, such as EPL, EP-LAN, and so on
- Step 7** In the Classification field, indicate what method will be used to identify and classify the traffic, then enter the relevant values in the Match Criteria field for the required bandwidth profiles:
- DSCP—Differentiated service code point (DSCP) value will be used to classify the traffic. Valid values are from 0 to 63. Up to 8 comma-separated values can be entered.
  - COS (Class of service)—Also known as PCP—IEEE 802.1Q bits in the header of the layer 2 frame from hosts supporting FCoe and other trunked devices. Valid values are from 0 to 7. Multiple comma-separated values or a range of values indicated by a hyphen (e.g., 0-2), can be entered.
- Step 8** Select one or more classes of service that will apply to the service.
- Step 9** For each class of service you selected, define a bandwidth profile to specify the match criteria and how the matching traffic will be handled. For each bandwidth profile, enter the match criteria, as described in [Step 7](#) above.

- Step 10** For each bandwidth profile, create rules to specify how the matching traffic will be handled. You can create a separate rule for ingress and egress traffic or you can create a rule for traffic moving in both directions. In each rule, you can specify the following:
- Committed Information Rate (CIR)—The long-term average transmission rate, specified in bits per second (bps).
  - Committed Burst Size (CBS)—How large traffic bursts can be (in bytes) before some traffic exceeds the CIR.
  - Excess Information Rate (EIR)—The average rate up to which packets are admitted. The EIR is greater than or equal to the CIR. Packets that exceed the CIR are typically discarded.
  - Excess Burst Size (EBS)—How large traffic bursts can be (in bytes) before traffic exceeds the EIR.
  - Color Mode—Specify whether traffic coloring will be applied or not.
- Step 11** Click **Submit** when you have defined all the required bandwidth profiles. Your QoS profile will be created and will be available for selection when you are creating VCs.
- 

## Create Customers

Customers must be created in the system so that they are available for selection during the circuit/VC provisioning process.

To create a customer:

- 
- Step 1** From the left sidebar, choose **Inventory > Other > Customers**.
- Step 2** Click **Create Customer**.
- Step 3** Enter the name of the customer and a description (optional).
- Step 4** Click **OK**. The customer is now added to the table of customers. You can select a customer to edit or delete it.
- 

## Provision a Circuit/VC with an Unmanaged Endpoint

You can create and provision a circuit/VC even if one or more of the endpoints is a device that is not managed by Cisco EPN Manager. The Provisioning Wizard allows you to identify an endpoint device as "unmanaged" and to provide information about that device so that the system can create the circuit/VC. Once you identify the unmanaged device, it will be available in the system in the Unmanaged Devices group and can be used for other services.

- 
- Step 1** Start the circuit/VC creation process for the required technology, as described in [Provision Circuits/VCs, on page 431](#).
- Step 2** For a point-to-point EVC and a CEM service:
- a) When defining the Z endpoint, select the **Unmanaged Device** check box. The Unmanaged Device Details panel opens.
  - b) If the unmanaged device has already been identified in the system, deselect the **New Device** check box and select the required device from the list. If you are identifying a new unmanaged device, provide the device name, IP address, and LDP IP. The LDP IP is used as the neighbor address of the pseudowire on the managed device.
  - c) Under Service Endpoint details, specify the virtual circuit identifier (VC ID). The VC ID field will be populated with the value of the VPN ID specified in the service details and will not be editable.

- Step 3** For a point-to multipoint or multipoint -to-multipoint EVC: In the Unmanaged UNI page, click the Plus icon in the table to add a row and then define the Unmanaged Device Details and Service Endpoint details for the selected row.
- Step 4** Complete the circuit/VC creation and provisioning process for the required technology, as described in [Provision Circuits/VCs, on page 431](#).

## Extend a Circuit/VC Using Templates

When you create and provision a circuit/VC, Cisco EPN Manager configures a set of CLI commands on the participating devices. If you need to configure additional commands on the same devices, you can create a template containing these commands and you can include it during the circuit/VC creation process. This effectively extends the circuit/VC beyond what is configured by Cisco EPN Manager. This functionality is available in the provisioning wizard but it is dependent on the template being created prior to creating or modifying the circuit/VC.

Extending a circuit/VC using CLI templates involves the following steps:

1. Create the CLI template using blank templates or existing templates. See [Create a New CLI Configuration Template Using a Blank Template, on page 384](#) and [Create a New CLI Configuration Template Using An Existing Template, on page 385](#).
2. Create/modify a circuit/VC and append the CLI template. See [Provision Circuits/VCs, on page 431](#).

- Step 1** Create the CLI template:
- a) In the left sidebar, choose **Configuration > Templates > Features & Technologies**.
  - b) In the Templates panel, choose **CLI Templates > CLI**.
  - c) Provide identifying information for the new circuit and define the content of the template using CLI, global variables, and/or template variables. See [Collect a Device's Inventory Now \(Sync\)](#) and [Use Global Variables in a Template, on page 390](#).
  - d) Click **Save as New Template**.
  - e) The new CLI template is saved under **My Templates > CLI Templates (User Defined)**.
- Step 2** Create/modify a service that includes the template you created (or a different template if relevant):
- a) From the left sidebar, choose **Maps > Topology Maps > Network Topology**.  
The network topology window opens.
  - b) Click the **Circuits/VCs** tab.
  - c) From the **Circuits/VCs** pane toolbar, either click the + (**Create**) icon or select a circuit and then click the pencil (**Modify**) icon.  
The Provisioning Wizard opens in a new pane to the right of the map.
  - d) Start creating or modifying the required circuit or VC. See [Provision Circuits/VCs, on page 431](#) and [Modify a Circuit/VC, on page 540](#).
  - e) In the **Service Template** page, use the **Pre-Configuration** section if you want the template to be a prefix to the service configuration or use the **Post-Configuration** section if you want the template to be a suffix to the service configuration.
  - f) In the **Template** drop-down menu, select the required CLI template.

The same CLI template cannot be selected for both pre-configuration and post-configuration options.

- g) In the **Template Usage** drop-down menu, select an option to indicate under what circumstances the CLI template should be configured on the devices. For example, if you select **Service Create Only**, the template CLI will only be configured on the devices when the service is created. It will not be configured when the service is modified.
- h) Enter values for the template parameters. The parameters shown here depend on the variables that were defined for the template.
- i) Click **Submit**.

**Note** By default, the selected CLI templates are associated with all devices that take part in the service. You cannot specifically choose the devices to be associated with the CLI templates.

## Example Configuration: Extend a Circuit/VC Using CLI Templates

**Example Configuration 1:** Extending an L3VPN service on a Cisco ASR 903 device using a CLI template with Global and Template (Local) variables:

```
vrf definition Testdoc1
exit
vrf Testdoc1
  vpn id 36B:3
  address-family ipv4 unicast
    import route-target
      65:1
    export route-target
      65:1
  address-family ipv6 unicast
    import route-target
      65:1
    export route-target
      65:1
interface GigabitEthernet0/0/0/11.2
  vrf Testdoc1
  ipv4 address 4.5.7.8 255.255.255.0
  mtu 1522
router bgp 140
  vrf Testdoc1
    rd auto
    address-family ipv6 unicast
    address-family ipv4 unicast
      redistribute static metric 54
    neighbor 3.4.6.8
      remote-as 21
    address-family ipv4 unicast
      exit
    exit
  exit
exit
interface GigabitEthernet0/0/6
  desc postconfig
  delay 5988
  mtu 436
  exit
```

**Example Configuration 2:** Extending a CEM service using a CLI template with a global variable and a template (local) variable:

```
#set($interfaceNameList = $gv.service-cem-cemInterfaceNameList.split(","))
#set($cemGroupNumberList = $gv.service-cem-cemGroupNumberList.split(","))
#set($count = 0)
#foreach($interfaceName in $interfaceNameList)
    interface $interfaceName
        service-policy input MainInterfacePolicy
        #if($count == 0)
            cem $cemGroupNumberList[0]
        #else
            cem $cemGroupNumberList[1]
        #end
        service-policy input servicePolicy
        #set($count = $count+1)
    #end
#end
```

### Example Configuration 3: Extending a CEM service to configure QoS over CEM:

```
#set($count = 0)
#foreach($interfaceName in $gv.service-cem-cemInterfaceNameList)
    interface $interfaceName
        service-policy input MainInterfacePolicy
        #if($count == 0)
            cem $gv.service-cem-cemGroupNumberList[0]
        #else
            cem $gv.service-cem-cemGroupNumberList[1]
        #end
        service-policy input servicePolicy
        #set($count = $count+1)
    #end
#end
exit
```

**Example Configuration 4:** Extending a CE service using a CLI template with global and template variables on a Cisco ME3800 device. The highlighted text represents the pre-config and post-config configuration changes that are appended and prepended to the CE service provisioning configuration.

```
pseudowire-class PWClass_51_192-168-12-29
protocol ldp
exit
ethernet cfm domain EVC level 4
    service evplextnpseudowireclass_ evc evplextnpseudowireclass_
        continuity-check
        continuity-check interval 1s
ethernet evc evplextnpseudowireclass
interface GigabitEthernet0/11
    no shutdown
    no spanning-tree portfast
    mtu 1522
    ethernet uni id 3800x
    service instance 1 ethernet evplextnpseudowireclass
        encapsulation dot1q 88
        xconnect 192.168.12.29 51 encapsulation mpls pw-class PWClass_51_192-168-12-29
        mtu 1508
    service instance 1 ethernet evplextnpseudowireclass_
        cfm mep domain EVC mpid 2
        ethernet lmi ce-vlan map 88
ip sla 17
    ethernet y1731 loss SLM domain EVC evc evplextnpseudowireclass_ mpid 1 cos 5 source mpid 2
    history interval 5
    aggregate interval 60
ip sla schedule 17 life forever start-time after 00:02:00
interface GigabitEthernet0/11
```



```
desc postconfig
exit
```

**Example Configuration 5:** Extending a Layer 3 Link service using a CLI template with a global variable and a template (local) variable:

```
##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
"MODIFY")
  ##XE DEVICE
  #if($variant=="IOS-XE")
  #if($gv.service-l3Link-routingProtocolName=="BGP")
    router bgp $gv.service-l3Link-routerProcessId
      address-family ipv4
        neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
      ##assume A End as remote building
      #if($gv.service-l3Link-isRouteReflectorClient=="TRUE" && $prefixListName!="" &&
$gv.service-l3Link-endPointDesignation=="AEND")
        neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list send
        neighbor $gv.service-l3Link-bgpNeighborName prefix-list $prefixListName
      in
        #elseif($gv.service-l3Link-isRouteReflectorClient=="TRUE" &&
$prefixListName!="" && $gv.service-l3Link-endPointDesignation=="ZEND")
        neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list receive
      #end
    exit
  exit
#end

  #if($xeMTU!="" || $xeClnsMTU!="")
  interface $gv.service-l3Link-interfaceName
    #if($xeMTU!="")
      mtu $xeMTU
    #end
    #if($xeClnsMTU!="")
      clns mtu $xeClnsMTU
    #end
    exit
  #end

  #if($gv.service-l3Link-routingProtocolName=="BGP")
  #if($addressFamily !="" && $addressFamily=="vpnv4")
    router bgp $gv.service-l3Link-routerProcessId
      address-family $addressFamily
        neighbor $gv.service-l3Link-bgpNeighborName activate
        neighbor $gv.service-l3Link-bgpNeighborName send-community both
      #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
        neighbor $gv.service-l3Link-bgpNeighborName route-reflector-client
      #end
      bgp additional-paths install
      neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
    exit
  exit
#end
#end
##XR DEVICE
#else

  #if($xrMTU!="")
  #if($gv.service-l3Link-subInterfaceName!="")
    interface $gv.service-l3Link-subInterfaceName
      mtu $xrMTU
    exit
  #else
```

```

        interface $gv.service-l3Link-interfaceName
            mtu $xrMTU
            exit
        #end
    #end

    #if($gv.service-l3Link-routingProtocolName=="BGP")
    #if($addressFamily != "" && $addressFamily=="vpnv4")
        router bgp $gv.service-l3Link-routerProcessId
            address-family $addressFamily unicast
        additional-paths receive
            exit
        neighbor $gv.service-l3Link-bgpNeighborName
            address-family $addressFamily unicast
            #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
                route-reflector-client
            #end
        aigp
            #if( $routePolicyName!="")
                route-policy $routePolicyName in
            #end
            exit
        exit
    #end
    #end

#end

##DELETE USE CASE
#elseif($gv.service-serviceOperationType == "DELETE")
##XE DEVICE
#if($variant=="IOS-XE")

    #if($xeMTU!=" " || $xeClnsMTU!="")
        interface $gv.service-l3Link-interfaceName
            #if($xeMTU!="")
                no mtu $xeMTU
            #end
            #if($xeClnsMTU!="")
                no clns mtu $xeClnsMTU
            #end
            exit
        #end

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily != "" && $addressFamily=="vpnv4")
            router bgp $gv.service-l3Link-routerProcessId
                no address-family $addressFamily
            exit
        #end
        #end

##XR DEVICE
#else
    #if($xrMTU!="")
        #if($gv.service-l3Link-subInterfaceName=="")
            interface $gv.service-l3Link-interfaceName
                no mtu $xrMTU
            exit
        #end
    #end
#end

```

```

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily != "" && $addressFamily=="vpnv4")
        router bgp $gv.service-l3Link-routerProcessId
        address-family $addressFamily unicast
        no additional-paths receive
        exit
        neighbor $gv.service-l3Link-bgpNeighborName
        no address-family $addressFamily unicast
        exit
        exit
    #end
    #end

#end

#end

```

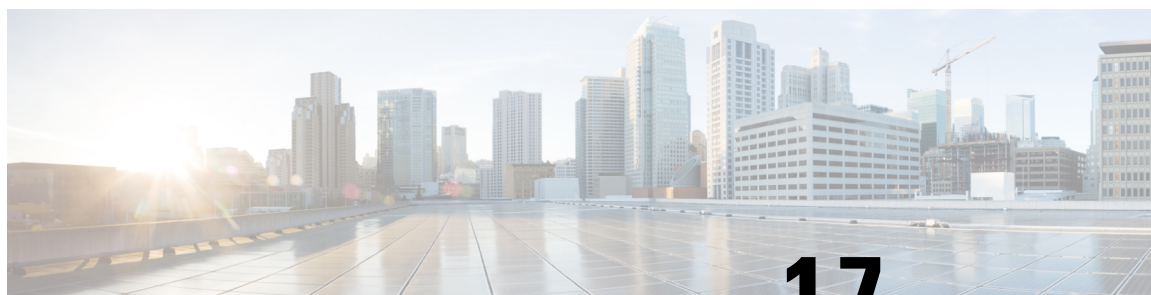
**Example Configuration 6:** Extending a Bidirectional TE tunnel using a CLI template with a global variable and a template (local) variable:

```

##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
"MODIFY")
    #if($variant && $variant=="IOS-XE")
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
            #if($xeBandWidth && $xeBandWidth!="")
                interface Tunnel$gv.service-teTunnel-tunnelId
                bandwidth $xeMaxBandWidth
                tunnel mpls traffic-eng auto-bw frequency $xeBandWidth max-bw
$xeMaxBandWidth min-bw $xeMinBandWidth
                exit
            #end
        #end
    #else
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
            #if($xrBandWidth && $xrBandWidth!="")
                interface tunnel-te$gv.service-teTunnel-tunnelId
                bandwidth $xrMaxBandWidth
                auto-bw
                bw-limit min $xrMinBandWidth max $xrMaxBandWidth
                application $xrBandWidth
                exit
            #end
        #end
    #elseif($gv.service-serviceOperationType == "DELETE")
        #if($variant && $variant=="IOS-XE")
            #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
                #if($xeBandWidth && $xeBandWidth!="")
                    interface Tunnel$gv.service-teTunnel-tunnelId
                    no bandwidth
                    no tunnel mpls traffic-eng auto-bw
                    exit
                #end
            #end
        #else
            #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
                #if($xrBandWidth && $xrBandWidth!="")
                    interface tunnel-te$gv.service-teTunnel-tunnelId
                    no bandwidth
                    no auto-bw
                    exit
                #end
            #end
        #end
    #end

```

```
        #end
    #end
#end
```



## CHAPTER 17

# View and Manage Discovered/Provisioned Circuits/VCs

---

- [Enable and Disable Service Discovery, on page 519](#)
- [Circuit or VC States, on page 520](#)
- [View Circuits/VCs, on page 525](#)
- [Filter and Export the Circuit/VC list Based on a User Defined Field, on page 538](#)
- [Display the Routes Associated With a Circuit, on page 539](#)
- [Promote a Discovered Circuit/VC Before Modifying/Deleting, on page 539](#)
- [Modify a Circuit/VC, on page 540](#)
- [Activate a Circuit \(Optical\), on page 541](#)
- [Restore a Circuit \(Optical\), on page 541](#)
- [Reroute a Circuit \(Optical\), on page 542](#)
- [Compare and Reconcile Provisioned and Discovered Versions of a Circuit/VC, on page 543](#)
- [Initiate a Protection Switch Action on a Circuit \(Optical\), on page 544](#)
- [Delete a Circuit/VC, on page 546](#)
- [Delete an L3VPN Service , on page 547](#)
- [Delete an L3VPN Service Endpoint, on page 548](#)
- [Delete an MPLS TE Service, on page 548](#)
- [Manage Provisioned Network Interfaces, on page 549](#)

## Enable and Disable Service Discovery

Cisco EPN Manager uses the service discovery feature to automatically discover the circuits/VCs existing in the network and the circuits/VCs that are provisioned using the Provisioning Wizard. The service discovery feature is enabled by default. You can choose to disable this feature. If you disable service discovery, all the discovered services in Cisco EPN Manager will be removed. However, the services that were provisioned using Cisco EPN Manager will remain and their state will be 'Missing'. You must restart the server to apply the changes.

To disable service discovery:

- 
- Step 1** From the left side bar, choose **Administration > Settings > System Settings**, then choose **Circuits/VCs > Discovery Settings**.

**Step 2** Uncheck the **Enable Service Discovery** check box.

**Step 3** Restart Cisco EPN Manager to apply your changes. See [Stop and Restart Cisco EPN Manager](#), on page 647







## Circuit or VC States

**Circuit or VC Primary States**— Conveys the most important state information for a circuit, in this order: Serviceability, Discovery, Alarm, Provisioning. It is normally shown in the first column of a circuit or VC table.

Circuit or VC Primary State	Icon	Serviceability	Discovery	Alarm	Provisioning
Missing		—	Missing	—	—
Down		Down	—	—	—
Critical		—	—	Critical	—
Major		—	—	Major	—
Minor		—	—	Minor	—
Partially Down		Partial	—	—	—
Admin Down		Admin Down	—	—	—
Partially Discovered		—	Partial	—	—
Failed		—	—	—	(Create, modify, or delete) failed
In progress		—	—	—	(Create, modify, or delete) in progress
Warning		—	—	Warning	—
Up		Up	—	—	—
Auto Up		Auto Up	—	—	—
Info		—	—	Info	—
Cleared		—	—	Cleared	—

**Circuit or VC Serviceability State**— This value is a combination of the circuit or VC's admin and operational states. The admin state is shown because it impacts service operability. For optical circuits, the admin state

also determines whether the Activate and Deactivate actions are available. The operational state is shown to quickly identify whether a service is working or not.

Circuit or VC Serviceability State	Icon	Description
Admin Down		Circuit or VC manually shut down by the administrator.
Down		Circuit or VC is operationally down and administratively up.
Up		Circuit or VC is operationally and administratively up.
Auto Up		Circuit or VC is operationally auto up and administratively up. Only certain devices support the Auto Up operational state.
Unavailable		Circuit or VC has not been discovered yet, or its operational status is unavailable.
Partial		<p>Circuit/VC operational or administrative state is partial.</p> <ul style="list-style-type: none"> <li>• Partial admin state—The circuit or VC has a mixed administrative request (to activate some service resources and deactivate others), has a mix of resources that are administratively up and down, or has resources whose operational state is unavailable.</li> <li>• Partial operational state—The circuit or VC has a mix of some active and deactivated resources, or the operational state for some of its resources are unavailable.</li> </ul>

Following table provides details of the serviceability states of Circuits/VCs under various scenarios:

Technology	Service Type	Scenario	Serviceability State
------------	--------------	----------	----------------------

Carrier Ethernet	EPL, EVPL, Access EPL, and Access EVPL	If the operational state of the endpoints (service instance / sub-interface), cross connects, and pseudowire participating in the service is up	Up
		If the admin state of both, the source and destination endpoints (service instance / sub-interface) participating in the service is down	Admin Down
		In all the other scenarios, when at least one endpoint (service instance / sub-interface), cross connect, or the pseudowire participating in the service is down	Down
	EP-LAN, EVP-LAN, EP-Tree, and EVP-Tree	If all the endpoints (service instance / sub-interface), bridge domains, VFIs, and pseudowires participating in the service are up	Up
		If the operational state of at least two endpoints (service instance / sub-interface) participating in the service are up and the rest of the endpoints are down	Partial
		If the admin state of all the endpoints (service instance / sub-interface) participating in the service is down	Admin Down
		If the operational state of at least one endpoint (service instance / sub-interface) participating in the service is up and the rest of the endpoints are down	Down



Circuit Emulation	All service types	If the operational state of the endpoints (cemGroup), underlying TDM controller, cross connect, and pseudowire participating in the service are up	Up
		If the admin state of both, the source and destination endpoints (cemGroup) participating in the service is down	Admin Down
		In all the other scenarios, when the operational state of one of the endpoint (cemGroup), underlying TDM controller, cross connect, and pseudowire participating in the service is down	Down
MPLS	Unidirectional TE Tunnel	If the operational state of the tunnel interface is up	Up
		If the admin state of the tunnel interface is down	Admin Down
		In all the other scenarios, when the operational state of the tunnel is down	Down
	Bidirectional TE Tunnel	If the operational states of the interfaces on both ends of the tunnel is up	Up
		If the admin states of the interfaces on both ends of the tunnel is down	Admin Down
		In all the other cases, when the operational state of the tunnel interface is down	Down





Layer 3 VPN		If the operational state of all the endpoints (sub-interface, BDI, and BVI) participating in the service is up	Up
		If the operational state of at least two endpoints (sub-interface, BDI, and BVI) participating in the service are up and the rest of the endpoints are down	Partial
		If the admin state of all the endpoints (sub-interface, BDI, and BVI) participating in the service is down	Admin Down
		If the operational state of at least one endpoint (sub-interface, BDI, and BVI) participating in the service is up and the rest of the endpoints are down	Down

**Circuit or VC Discovery State**—Represents the latest state and structure of a service and its components, as discovered from the network. Having a Discovered version means that the application is actually monitoring the service itself, e.g. it can define meaningful operational and performance data.

Circuit or VC Discovery State	Icon	Description
Partial		Circuit or VC partially discovered by Cisco EPN Manager ; not all of its expected entities have been discovered.
Full		Circuit or VC fully discovered by Cisco EPN Manager , so Cisco EPN Manager can monitor the service and provide meaningful operational and performance data.
Missing		Circuit or VC not yet discovered by Cisco EPN Manager (though it may have been provisioned).

**Circuit or VC Provisioning State**—Represents whether there is a provisioning intent for a circuit or VC and, if so, its status. If a reconciliation report has been generated, the state of the reconcile action is reflected.

Circuit or VC Provisioning State	Icon	Description
None		Circuit or VC was discovered but has not yet been provisioned. The circuit/VC must be promoted in order to modify or delete it.

Failed		Action has failed.
In Progress		Action was initiated but not yet completed.
Planned		Action is planned but not yet initiated.
Succeeded		Action has completed successfully.

## View Circuits/VCs

Cisco EPN Manager provides a variety of ways that you can view circuits/VCs:

To view circuit/VC information for:	See the procedures in:
A specific circuit/VC in a topology map, in a Circuit/VC 360 view, or in a Circuit/VC Details page	<ul style="list-style-type: none"> <li>• <a href="#">Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 528</a></li> <li>• <a href="#">Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 532</a></li> </ul>
A device	<a href="#">View a Specific Device's Circuits/VCs, on page 534</a>
A device group in a topology map or in an expanded table	<a href="#">View a Device Group's Circuits/VCs, on page 535</a>
All of Cisco EPN Manager	<a href="#">View All Circuits/VCs in Cisco EPN Manager , on page 536</a>

## View a Specific Circuit/VC's Details

Cisco EPN Manager provides different ways to view details about a specific circuit/VC, depending on how much detail you need:

- [View a Specific Circuit/VC in the Topology Map, on page 525](#)
- [Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 528](#)
- [Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 532](#)
- [View and Compare Versions of a Circuit \(Optional\), on page 533](#)

## View a Specific Circuit/VC in the Topology Map

When working with circuits/VCs, it is very useful to see how a circuit/VC is deployed within the existing network topology. Cisco EPN Manager overlays the circuit/VC on an existing topology map, clearly indicating the endpoints and midpoints of the circuit/VC, the role of the endpoint (where relevant), and relevant fault information for the circuit/VC. This overlay functionality is available in the geo map as well as the topology map.

For CE and CEM services that use the MPLS TE tunnels to traverse through the network, the underlying tunnel is also displayed in the topology map along with the service overlay. For information about how to

assign a MPLS TE tunnel for a CE or CEM service, see [Provision EVCs in a Carrier Ethernet Network](#), on page 436 and [Provision Circuit Emulation Services](#), on page 483 .



#### Note

- The overlay cannot be displayed if the discovery state of the circuit is "Missing".
- A circuit/VC might contain endpoints that cross device groups, meaning that one endpoint might belong to one group and another might belong to a different group. In this case, the full overlay cannot be shown. If an endpoint is not currently shown in the map, a notification link will appear at the top left of the map. Click the link to expand the map to show all the device groups that contain endpoints of the selected circuit/VC.
- When the overlay is displayed, the Link Type filter is disabled.











To display an overlay of a circuit/VC on the network topology:



- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click the **Device Groups** button and select the required group.
- Step 3** Go to the **Circuits/VCs** tab to see a list of the circuits/VCs associated with the selected group.
- Step 4** Select the circuit/VC you want to see on the map.

The nodes and links that participate in the selected circuit are highlighted in the overlay and the rest of the devices in the map appear disabled. The name of the selected circuit is displayed just below the topology toolbar. To clear the overlay,

click the 'x' button to the right of the circuit name. For a description of the overlay icons, see [Circuit or VC Network Topology Overlay Icons](#).

### Circuit or VC Network Topology Overlay Icons

Overlay Icon	Definition
	Source endpoint
	Destination endpoint
	EVC or CEM service with local switching
	Endpoint included by the user during creation of the circuit.
	Endpoint excluded by the user during the creation of the circuit.
	Endpoint with some ports that were either included or excluded during creation of the circuit. This endpoint contains multiple ports that are participating in various routes of the circuit.
	E-TREE EVC endpoint that has been designated as a root.
	Selected endpoint.
	Hub; If the hub and root are on the same device (VPLS scenario), the brown circle is combined with the root icon.
	Link included during creation of the circuit.

Overlay Icon	Definition
	Link excluded during creation of the circuit.
	Endpoint with some ports that were either included or excluded during creation of the circuit. This represents the aggregated link that contains multiple ports participating in various routes of the same circuit.

## Get Quick Information About a Circuit/VC: Circuit/VC 360 View

The Circuit/VC 360 view provides at-a-glance information about a specific circuit/VC. From the Circuit/VC 360 view, you can access detailed information about the circuit/VC and perform the actions described in [Actions You Can Perform from the Circuit/VC 360 View, on page 530](#).

The Circuit/VC 360 view displays the circuit name, state, and general circuit/VC and performance information at the top of the view. More detailed information is provided in tabs in the lower part of the view.

Information Provided in Circuit/VC 360 View	Description
General information	<p>Type of circuit/VC, its various states (discovery, serviceability, provisioning), the customer associated with the circuit/VC, and some audit information (when it was created, when it was last changed). For an explanation of circuit/VC states, see <a href="#">Circuit or VC States, on page 520</a>.</p> <p><b>Note</b> If the Provisioning state is <b>Create Failed</b>, click the associated <i>i</i> (<b>information</b>) icon to see the reason for the failure.</p>
Performance data	<p>Graphs reflecting various aspects of the circuit/VC performance.</p> <p><b>Note</b> For data to be shown in the graphs, the required monitoring policy must be activated for the relevant devices. For example, to view graphs that chart the number of Explicit Pointer Adjustment Relay counters (such L-bits and P-bits) that have been generated and received, both the CEM and Pseudowire Emulation Edge to Edge monitoring policies must be enabled. See <a href="#">Monitoring Policies Reference, on page 767</a>.</p>
Alarms	Current alarms for the circuit/VC, including their severity, status, and the time they were generated.
Endpoints	Devices and interfaces that serve as endpoints for this circuit/VC.

History	<p>The <b>History</b> tab lists all versions of the circuit, allowing you to view the changes that have occurred since the circuit/VC was discovered or first deployed. You can open the Circuit 360 view for any of the versions listed to see its endpoints, alarms, and so forth.</p> <p><b>Note</b> If you are looking at the Circuit 360 view for a historical circuit/VC, the <b>History</b> tab is not displayed.</p> <p>You can also view the configuration details for the circuit/VC's endpoints by doing the following:</p> <ol style="list-style-type: none"> <li>1. Locate the appropriate circuit/VC version and click its <i>i</i> (<b>information</b>) icon in the <b>Provisioning State</b> column. The <b>Device Configuration Details</b> pop-up window opens.</li> <li>2. Click the radio button for the endpoint whose configuration details you want to view. If the endpoint was successfully provisioned, its configuration is listed at the bottom of the pop-up window. If provisioning of the endpoint failed, a description of why provisioning failed is listed instead.</li> </ol>
Related Circuits/VCS	Additional circuits within the selected circuit.

For EVCs, the following information is shown:

- **Incoming Traffic**—The sum of incoming traffic, in bits per second (bps), entering all the endpoint interfaces of the circuit/VC over time. The graph shows the last 24 samples of the total incoming traffic for all the endpoints in intervals of 1 minute. The pink bar shows the lowest level of incoming traffic while the blue bar shows the highest level of incoming traffic.
- **Port Availability**—Average availability of all the endpoints of the circuit/VC, expressed as a percentage, aggregated across all endpoints. Baseline is 100% unless any of the interfaces has been unavailable.
- **Outgoing Traffic**—The sum of traffic, in bits per second (bps), exiting all the endpoint interfaces of the circuit/VC over time.
- **Loss**—Average loss, expressed as a percentage, across all the endpoints of the circuit/VC.
- **Delay**—Average delay, in microseconds, across all the endpoints of the circuit/VC.
- **Jitter**—Average jitter, in milliseconds, across all the endpoints of the circuit/VC.

For optical circuits, the performance data is shown based on the following circuit types:

- **OCHCC WSON**—The total number of octets received on the interface, including frames, number of inbound packets with errors that prevented them from being delivered to a higher layer protocol, and number of severely errored seconds per line and multiplex sections.
- **OCHNC WSON**—The average, minimum, and maximum optical signal to noise ratio (OSNR) for this circuit type.
- **OCH-TRAIL WSON**—The total number of uncorrectable words and the total number of errors corrected, in bits per second (bps), for this circuit type.
- **OCH-Trail UNI**—The total number of uncorrectable words and the total number of errors corrected, in bits per second (bps), and the minimum, average, and maximum output power received and transmitted, in decibel referenced to 1 watt (dBW) by this circuit type.
- **ODU UNI**—The total number of background block errors, total number of severely errored seconds, and errored seconds ratio for path monitoring.

- ODU Tunnel—The total number of background block errors, total number of severely errored seconds, and errored seconds ratio for section monitoring.

In addition, the average, minimum, and maximum amount of output power received and transmitted from the circuit is shown for all optical circuit types.

For Circuit Emulation services, the following information is shown:

- The total number of jitter buffer overruns for each circuit endpoint.
- The total number of Explicit Pointer Adjustment Relay counters (such as L-bits and R-bits) that were generated and received for each circuit endpoint.

For services on a Cisco ME 1200 device, information such as incoming and outgoing traffic, jitter, and availability is displayed.

For MPLS bidirectional TE tunnels, ensure that you activate the Interface Health monitoring policy so that the performance data is shown. See [Monitoring Policies Reference, on page 767](#) for more information. The following performance data is shown:

- Traffic—The sum of traffic in both directions of the tunnel, in bits per second (bps).
- Availability—Average availability of the endpoints in the tunnel.
- Bandwidth Utilization—The percentage of bandwidth configured on the tunnel against the sum of the percentage of bandwidth configured on all the pseudowires associated with the tunnel.
- Actual Bandwidth Utilization—The percentage of bandwidth configured on the tunnel against the sum of the percentage of bandwidth utilized for the incoming and outgoing traffic in all the pseudowires associated with the tunnel.

To open the **Circuit/VC 360** view for a particular circuit or VC:

---

**Step 1** Choose **Maps > Topology Maps > Network Topology**.

The network topology window opens. See [Visualize the Network Topology, on page 149](#) for a description of the network topology window and its functionality.

**Step 2** From the **Network Topology** page toolbar, click **Device Groups**.

The **Device Groups** pop-window opens.

**Step 3** Locate and click the device group that the circuit or VC is associated with, then close the pop-up window.

**Step 4** Click the **Circuits/VCs** tab.

**Step 5** Locate the circuit or VC in the list and then click its *i* (**information**) icon.

---

## Actions You Can Perform from the Circuit/VC 360 View

The following is a list of the actions you can perform from the **View** and **Actions** menus for the selected circuit or VC. The actions that are available will vary, depending on the type of circuit or VC that is selected:

- Choose **View > Details** to display further details about the circuit/VC. See [Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 532](#).
- Choose **View > Service Trace** to trace the route of an optical circuit. See [Trace and Visualize the Full Route of a Circuit, on page 172](#).
- Choose **View > Dashboard** to view the service performance dashboard of the circuit/VC. See [Set Up and Use the Dashboards, on page 6](#).



- Choose **Actions** > **Add to Compare** to select the circuit or VC for a side-by-side comparison with another circuit or VC on the basis of information such as serviceability and provisioning state and raised alarms. See [Compare Circuit/VC Information and Status](#).
- Choose **Actions** > **Multilayer Trace** to visualize a circuit in a graphical manner. See [Trace and Visualize the Full Route of Circuits/VCs](#).
- Choose **Actions** > **Y.1564 Test** to test the performance of the CE circuit/VC end to end. See [Running a Y.1564 Performance Test, on page 560](#).
- Choose **Actions** > **BER Test** to test the performance of the Circuit Emulation Services. See [Performance Test for Circuit Emulation Services, on page 565](#).
- Choose **Actions** > **Optical PM Parameters** to view the realtime performance monitoring data of the optical circuit/VC. See [Optical Performance Monitoring Parameters, on page 563](#).
- Choose **Actions** > **PRBS Test** to test the performance of the optical circuit/VC end to end. See [Run PRBS Test on Circuits \(ODU UNI\), on page 563](#).
- Choose **Actions** > **Restoration Actions** > **Upgrade Restore** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred. See [Restore a Circuit \(Optical\), on page 541](#).
- Choose **Actions** > **Restoration Actions** > **Manual Revert** to revert the optical circuit to its original route when the route is recovered from the failure. See [Restore a Circuit \(Optical\), on page 541](#).
- Choose **Actions** > **Reroute Actions** > **Working Path** or **Protected Path** to reroute the traffic through the working path or protected path defined for the circuit. See [Reroute a Circuit \(Optical\), on page 542](#).
- Choose **Actions** > **Activate** to allow the traffic to pass through the optical circuit. See [Activate a Circuit \(Optical\), on page 541](#).
- Choose **Actions** > **Deactivate** to stop the traffic passing through the optical circuit. See [Activate a Circuit \(Optical\), on page 541](#).
- Choose **Actions** > **OAM Commands** to troubleshoot a service failure using OAM commands. See [Troubleshoot a Service Failure Using OAM Commands, on page 554](#).
- Choose **Actions** > **Show in Topology** to view the circuit/VC overlay in the topology map.
- Click the *i* icon next to the Serviceability status to view additional information about a circuit failure. See [Get More Information About a Circuit/VC Failure, on page 553](#).

## Compare Circuit/VC Information and Status

From the **Comparison View**, you can perform a side-by-side comparison of multiple circuits or VCs, viewing information such as discovery and provisioning state, raised alarms, and associated endpoints. To compare circuits or VCs, do the following:

### Step 1

For each circuit or VC you want to compare:

- Open its **Circuit/VC 360** view, as described in [Get Quick Information About a Circuit/VC: Circuit/VC 360 View](#).
- Choose **Actions** > **Add to Compare**.

The circuit or VC you selected is displayed at the bottom of the page. You can select a maximum of 4 circuits and VCs.

### Step 2

Click **Compare**.

The **Comparison View** opens.

- Step 3** From the drop-down list at the top of the view, specify whether the view will show all available information or just the information that is unique to each device.
- Step 4** Click **Comparison View**, check the check box for the categories you want the view to display, and then click **Save**.  
By default, all of the categories are already selected.
- Step 5** Scroll down the page to view the information provided for each category you selected.

Note the following:

- The **Comparison View** only displays information for two circuits or VCs at a time. If you selected more than two, you will need to toggle to the circuits or VCs that are not currently displayed.
- To reorder the circuits or VCs you have selected, click **Rearrange**.
- Each circuit or VC's **View** and **Actions** menu is identical to the ones provided in its **Circuit/VC 360** view. If you select an option, the corresponding page opens.
- You can minimize and maximize the categories displayed, as needed.
- The **Comparison View** is also available for devices, interfaces, and links. Whenever you select any of these elements from their respective 360 view for comparison, they are displayed in the corresponding tab. This allows you to switch between element types, as needed.
- When you are done comparing circuits or VCs, click **Back** at the top of the view and then click **Clear All Items** at bottom of the page. If tabs for other element types are still displayed, you will need to clear them as well.

---

## Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window

The Circuit/VC Details window provides additional details about a specific circuit/VC, including the attributes defined for the circuit/VC. The information shown in the displayed page varies depending on the type of circuit/VC. You can also perform certain actions from the Circuit/VC Details Window, for example, modify/delete the circuit/VC, create a new circuit/VC, run a performance test.

To access the Circuit/VC Details window, click on the circuit/VC name hyperlink in any of the circuit/VC tables. Alternatively, you can access the Circuit/VC details window from the Circuit/VC 360 view, as follows:

- Step 1** Access the Circuit/VC 360 view for the required circuit/VC. See [Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 528](#).
- Step 2** Choose **View > Details**. See [Provision EVCs in a Carrier Ethernet Network, on page 436](#) and [Provision Circuits in an Optical/DWDM Network, on page 447](#) for description of the attributes in the Circuit/VC details page.

The details are displayed in two tabs:

- **Summary**: Displays circuit information such as the circuit discovery and provisioning states, acceptance threshold, WSON label, circuit type, wavelength associated with the circuit, protection status, and more.
  - **Ports**: Displays ports information such as the ports associated with the circuit, their port roles, the IP addresses associated with the ports, and more
-

## Actions You Can Perform from the Circuit/VC Details Page

From the Circuit/VC Details window, you can do the following:

- Modify the circuit/VC (action available for circuits/VCs provisioned using Cisco EPN Manager , not for discovered circuits/VCs). See [Modify a Circuit/VC, on page 540](#).
- Delete the circuit/VC (action available for circuits/VCs provisioned using Cisco EPN Manager , not for discovered circuits/VCs). See [Delete a Circuit/VC, on page 546](#).
- Create a new circuit/VC. Clicking the Create button opens the Provisioning Wizard, enabling you to create a new circuit/VC. See [Provision EVCs in a Carrier Ethernet Network, on page 436](#) and [Provision Circuits in an Optical/DWDM Network, on page 447](#).
- Choose **Actions** > **Y.1564 Test** to test the performance of the CE circuit/VC end to end. See [Running a Y.1564 Performance Test, on page 560](#).
- Choose **Actions** > **BER Test** to test the performance of the Circuit Emulation Services. See [Performance Test for Circuit Emulation Services, on page 565](#).
- Choose **Actions** > **Optical PM Parameters** to view the realtime performance monitoring data of the optical circuit/VC. See [Optical Performance Monitoring Parameters, on page 563](#).
- Choose **Actions** > **PRBS Test** to test the performance of the optical circuit/VC end to end. See [Run PRBS Test on Circuits \(ODU UNI\), on page 563](#).
- Choose **Actions** > **Restoration Actions** > **Upgrade Restore** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred. See [Restore a Circuit \(Optical\), on page 541](#).
- Choose **Actions** > **Restoration Actions** > **Manual Revert** to revert the optical circuit to its original route when the route is recovered from the failure. See [Restore a Circuit \(Optical\), on page 541](#).
- Choose **Actions** > **Activate** to allow the traffic to pass through the optical circuit. See [Activate a Circuit \(Optical\), on page 541](#).
- Choose **Actions** > **Deactivate** to stop the traffic passing through the optical circuit. See [Activate a Circuit \(Optical\), on page 541](#).

## View and Compare Versions of a Circuit (Optical)

Use the Circuit History page to compare two versions of an optical circuit. From the Circuit History page, you can:

- Get a simple visualization and integrated view of the events that occurred in the optical circuit.
- View the alarms associated with an event.
- Compare the route changes in the circuit.

For example, consider that there is a restoration that has occurred in an optical circuit. Using the Circuit History page, you can:

1. View the list of changes that had occurred in the circuit.
2. If there is a protection switch action that had occurred in the circuit, you can click the *i* icon in the Type column to see the details of the event that has caused the protection switch action.
3. Click the *i* icon in the Time Stamp column to see the alarms that are associated with the event.
4. You can further compare the route changes between the active path and the path at the time of protection switch.

5. You can also choose to compare the route changes between the active path and the original path or between the original path and the path at the time of protection switch to view the difference in the participating nodes and take action on the affected nodes.

To view the history of an optical circuit:

**Step 1** From the left side bar, choose **Maps > Topology Maps > Network Topology**.

**Step 2** Click **Device Groups**, and then select the location in which the required circuit/VC was created.

**Note** By default, **All Location** group is selected.

**Step 3** Close the **Device Groups** popup window.

**Step 4** In the **Network Topology** window, click **Circuits/VCs**.

**Step 5** Select the optical circuit for which you want to view the history. The overlay of the circuit is displayed on the map.

**Step 6** Click the **Circuit History** hyperlink that appears right below the topology toolbar.

The **Circuit History** area is displayed next to the topology map and lists the various versions of the circuit. The active route of the circuit is selected by default and it is displayed on the map.

**Step 7** Select a history version from the list displayed in the **Circuit History** area to compare it with the current version.

The overlay on the map changes based on your selection and displays both, the active route and the history version. You can select and compare only two versions at a time.



## View a Specific Device's Circuits/VCs

Use the Device 360 view to see a list of all the circuits/VCs in which a specific device participates. This is useful when a specific device is having a problem and you want to see which services it will affect.

To view a list of circuits/VCs in which a device participates:

- 
- Step 1** Click the required device in the network topology (**Maps > Topology Maps > Network Topology**).
- Step 2** Click **View 360** in the popup window.
- Step 3** Go to the Circuit/VC tab in the Device 360 view to see a table listing the relevant circuits for that device. The table lists the circuit/VC name, the circuit/VC type, when it was created/modified, and the current status of the circuit/VC.
- 

## View a Device Group's Circuits/VCs

- [View a Device Group's Circuits/VCs List in the Topology Window, on page 535](#)
- [View a Device Group's Circuits/VCs in an Expanded Table, on page 535](#)

### View a Device Group's Circuits/VCs List in the Topology Window

Cisco EPN Manager displays discovered and provisioned circuits/VCs in the Circuits/VCs tab on the left side of the network topology window. The list of circuits/VCs is filtered according to the selected device group. You can get details about the circuit/VC by clicking on the circuit/VC name to launch the Circuit/VC Details window or by clicking the information icon and launching the Circuit/VC 360 view.

The Circuits/VCs tab lists discovered circuits/VCs and the latest version of circuits/VCs provisioned using Cisco EPN Manager. The circuits/VCs are sorted by primary state (default).

To view a list of circuits/VCs in the network topology window:

- 
- Step 1** Choose **Maps > Topology Maps > Network Topology** in the left navigation pane. The network topology window opens.
- Step 2** Click the **Device Groups** button and select the group of devices you want to show on the topology map.
- Step 3** Go to the Circuits/VCs tab to see a list of circuits/VCs relevant to the selected device group.
- Step 4** Select a circuit/VC to view an overlay of the circuit/VC in the network topology, meaning that the circuit/VC endpoints and path are shown on top of the physical topology. Click on the circuit name hyperlink to see circuit details or click on the information icon next to the circuit/VC name to open the Circuit/VC 360 view.
- Step 5** To open a tabular view of the circuits/VCs in a separate window, click **Circuit/VCs** below the list of circuits/VCs.
- 

### View a Device Group's Circuits/VCs in an Expanded Table

From the network topology window, you can open a table of circuits/VCs associated with the selected device group in a separate browser window. The table provides more information about each circuit/VC and is also sortable and searchable, enabling you to find information easily. This table is particularly useful for identifying the provisioning status of circuits/VCs, as well as their management status within Cisco EPN Manager. For an explanation of circuit/VC states (and their icons, see [Circuit or VC States, on page 520](#)).

By default, the circuits/VCs table sorts the circuits/VCs by primary state. You can change how the table is sorted as required.

The expanded circuits/VCs table works together with the Network Topology window so that if you select a circuit/VC in the table, the circuit/VC will be represented graphically in the Network Topology window in the context of the topology map.

To open an expanded and more detailed tabular list of circuits in a separate window:

- 
- Step 1** Choose **Maps > Topology Maps > Network Topology** in the left navigation pane. The network topology window opens.
- Step 2** Click the **Device Groups** button and select the group of devices you want to show on the topology map.
- Step 3** Go to the Circuits/VCs tab to see a list of circuits/VCs relevant to the selected device group.
- Step 4** Click the **Circuit/VCs** hyperlink below the list of circuits/VCs to open a separate window containing a list of circuits/VCs relevant to the selected device group.
- 

- See more information about the circuit/VC by displaying the Circuit/VC 360 view. See [View Circuits/VCs, on page 88](#).
- View the circuit/VC on the map, as an overlay on top of the displayed devices. See [View a Specific Circuit/VC in the Topology Map, on page 525](#).
- Launch the Provisioning Wizard to provision circuits/VCs. See [Create and Provision a New Carrier Ethernet EVC, on page 437](#) and [Provision Circuits in an Optical/DWDM Network, on page 447](#).
- See more information about a circuit failure. See [Get More Information About a Circuit/VC Failure, on page 553](#).
- Select a circuit/VC for modification, deletion, circuit trace, and performance test. See the following topics for more information:
  - [Modify a Circuit/VC, on page 540](#)
  - [Delete a Circuit/VC, on page 546](#)
  - [Run a Performance Test on a Circuit/VC, on page 558](#)

## View All Circuits/VCs in Cisco EPN Manager

The **Circuits/VCs & Network Interfaces** page lists all of the circuits and VCs that Cisco EPN Manager is currently managing. From here, you can quickly locate a specific circuit or VC by filtering the list using basic criteria such as name, type, or customer. You can view the number of EFPs that Cisco EPN Manager has provisioned. If all the EFPs are provisioned, the number of EFPs will match the number of services. You can identify all of the circuits and VCs that have severe alarms or are in a specific state. (For a description of circuit and VC states (including primary states), see [Circuit or VC States, on page 520](#).) You can also perform circuit and VC management tasks and run performance tests. To use this page, do the following:




---

**Note** After a device that is participating in a circuit or VC is removed from Cisco EPN Manager, the corresponding circuit or VC is still listed on the **Circuits/VCs & Network Interfaces** page.

---

- 
- Step 1** Choose **Inventory > Other > Circuits/VCs & Network Interfaces**.
- Step 2** Perform any of the following actions:
- Find specific circuits or VCs by using one of the quick filter fields. For example, enter **L3VPN** in the **Type** field to list all circuits and VCs of that type or click the **Serviceability** quick filter field and then choose **Down** to view all circuits and VCs that are currently down.
  - View a specific circuit or VC in the topology map by clicking its radio button and then choosing **Actions > Show in Topology**.

- With a circuit or VC selected, use the **Actions** menu to activate circuits or VCs and run performance tests.
- Create, modify, or delete circuits and VCs by clicking the appropriate button in the **Circuits/VCs & Network Interfaces** page toolbar, which opens the provisioning wizard.

---

## Identify and Manage Discovered Circuits/VCs

Cisco EPN Manager discovers existing network circuits/VCs and displays them in the Circuit/VC list. Discovered circuits/VCs are automatically named by the system. The names for EVCs begin with **EvcLink\_** (for example, EvcLink\_Vpls\_Bridge\_318#318#VFIVPLS2\_541549\_10.56.23.48#1).



**Note** When circuits/VCs are discovered, the system identifies whether they are optical, CE, or L3VPN circuits/VCs, but it cannot identify the exact *type* of CE circuit/VC. For example, CE circuits/VC will display **EVC** in the Type column but not the type of EVC, such as EPL, E-LAN, and so on. For optical, the exact *type* of circuit is displayed.

You can do the following with discovered circuits/VCs:

- Identify discovered circuits/VCs in the Circuit/VC list by name or in the table of circuits/VCs by state, **Discovered**.
- View details about the discovered circuits/VCs in the Circuit/VC 360 view, including the endpoints of the circuit/VC.
- View an overlay of the circuit/VC on the network topology.
- View fault information for the circuit/VC.
- Promote a discovered circuit/VC, after which you can edit or delete it (applies to optical circuits and selected EVCs. See [Promote a Discovered Circuit/VC Before Modifying/Deleting, on page 539](#)).
- Do a performance test.

## Show/Hide Implicit Circuits

A circuit is classified as implicit if it is an underlying or "carrying" circuit of another circuit. For example, an OCHTRAIL circuit could be a carrying circuit (and implicit) for an OCHCC circuit. By default, all circuits are listed in the circuit lists. However, you can hide implicit circuits from the lists, if required. When implicit circuits are hidden, they will not be displayed in the circuit lists but you can see them in the Carrying Circuits tab of the Circuit 360 view.

To hide implicit circuits from the circuit lists:

- 
- Step 1** From the left sidebar, choose **Administration > Settings > System Settings**.
  - Step 2** From the System Settings menu, choose **Circuits/VCs > Circuits/VCs Display**.
  - Step 3** Uncheck the Show Implicit Circuits/VCs check box.
-



# Filter and Export the Circuit/VC list Based on a User Defined Field

You can create a user defined field, assign a value to the field, and associate it to a circuit/VC. You can then sort, filter, and export the circuit/VC list based on the user defined field.

For example, if you want to filter the circuit/VC list based on the service impact, you need to:

- Create a user defined field, named Service Impact
- Select the circuit/VC to which you want to associate the user defined field, Service Impact
- Assign the value as Critical, Moderate, or Low for the Service Impact field
- Sort, filter, and export the circuit/VC list based on the service impact value



**Note** You can create a maximum of 10 user defined fields.

**Step 1** To create a user defined field, do one of the following:

- Choose **Administration > Settings > System Settings > Inventory > User Defined Fields**, and then click the '+' icon to create a new label and description. Click **Save**.

**Note** You cannot assign a value to the user defined field from the **Administration** menu.

- Choose **Inventory > Other > Circuits/VCs & Network Interfaces**, select a circuit/VC, and then choose **Actions > Manage User Defined Fields**. Click the '+' icon to create a user defined field, its description, and value. Click **Save**.
- Choose **Maps > Topology Maps > Network Topology**, go to the **Circuits/VCs** tab, and then click the Circuits/VCs hyperlink below the list of circuits/VCs. An expanded table of circuits/VCs opens in a separate window. Select a circuit/VC, and then choose **Actions > Manage User Defined Fields**. Click the '+' icon to create a user defined field, its description, and value. Click **Save**.

**Step 2** In the Circuits/VCs & Network Interfaces page or in the expanded table of circuits/VCs, click the settings icon at the top right of the page, and then choose **Columns**.

**Step 3** Choose the user defined field you have created, and then click **Close**. The user defined field with the assigned value is displayed as a column in the table of circuits/VCs.

**Step 4** Click the Export icon next to the Settings icon at the top right of the table to export the data from the table to a file (either PDF or CSV format).

You can delete the user defined field only from **Administration > Settings > System Settings > Inventory > User Defined Fields**.



## Display the Routes Associated With a Circuit

Use the network topology **Routes** drop-down menu to display specific routes associated for a circuit in the circuit overlay. Cisco EPN Manager calculates the routes from the links within a service. You can also filter the overlay based on the selected routes.



**Note** This feature is supported only on point-to-point CE services, optical circuits, and CEM services.

- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** From Device Groups list, select the required group. Cisco EPN Manager lists the circuits associated with the selected group in the Circuit/VCs tab.
- Step 3** Click **Circuit/VCs**, and then select the circuit you want to display.
- Step 4** From the **Routes** drop-down list, choose the required route type.

**Note** The route types are based on the routes configured on the selected circuit.

## Promote a Discovered Circuit/VC Before Modifying/Deleting

Discovered circuits need to be promoted before they can be modified or deleted. After being promoted, the circuit/VC's provisioning state changes to Promote Successful.



**Note** Promotion is supported for Optical circuits and for basic EVCs that do not have additional configurations, such as CFM, LMI, QoS, OAM, G.8032, ICCP-SM. Promotion is supported if the underlying core is VPLS (for E-LAN and E-Tree EVCs). If a discovered circuit/VC cannot be promoted, it cannot be modified or deleted.

To promote a discovered circuit/VC:

### Before you begin

For successful promotion of L3VPN services, you must ensure that the route distinguisher for the L3VPN service is specified in the format **rd device\_ip:number**.

For example:

```
vrf definition vdvvgfr420
  rd 10.104.120.133:420
  vpn id 36B:420
  !
address-family...
```

- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**. The network topology window opens.

- Step 2** Click the **Device Groups** button and select the required group.
- Step 3** Go to the Circuits/VCs tab and click the **Circuits/VCs** link to open an extended table of circuits/VCs in the selected group.
- Step 4** Select the discovered circuit/VC you want to promote.
- To identify L3VPN services that are discovered from the device but not promoted, filter out L3VPN services that have the provisioning status 'None'. You can also identify discovered services using the Name field of the L3VPN service. The Name field for L3VPN services that are discovered are represented with the service's unique VLAN IDs.
- Step 5** Click **Modify**. The Provisioning Wizard opens.
- Step 6** For optical circuits, modify the circuit as required, then click **Create**.
- Step 7** For EVCs, do the following:
- In the Endpoints Details page, select an endpoint. Fields relevant to the selected endpoint are displayed below.
  - Specify the type of endpoint by selecting UNI or ENNI from the dropdown list, and enter a name for the endpoint. For UNIs, you can also set bundling and multiplexing attributes.
  - Select the next endpoint and define its type, name, and attributes.
  - Click **Next**.
  - In the Manage Discovered Service: Service Details page, select the Type of service. The available types in the list are derived from the types of endpoints and UNI options you defined. For example, if you defined a UNI with All to one Bundling option and an ENNI, only Access EPL will be available in the list. You can go back and redefine your endpoints if necessary.
  - Give the service a name. Provide a description and specify a customer, if required.
  - For E-Tree EVCs, specify the role of each endpoint (root or leaf) in the Endpoint Designation table. The role you specify here must match the role that is configured on the device.
  - Click **Save**. The EVC will appear with its new name in the Circuits/VCs list and its status will be Created and Deployed.
  - You can now select the promoted EVC in the list and modify or delete it.
- Step 8** For L3VPN services, do the following:
- Give the service a name. Provide a description and specify a customer, if required, and click **Next**.
  - In the **Deployment Action** drop-down menu, specify the task (Preview or Deploy) that must be taken up when the VPN service promotion process is completed, and click **Next**.
  - Specify the UNI name, the MTU value, and whether service multiplexing should be enabled.
  - Click **Save**. The L3VPN service will appear with its new name in the Circuits/VCs list and its status will be Promote Successful.
  - You can now select the promoted L3VPN service from the list and modify or delete it.

## Modify a Circuit/VC

You can modify circuits/VCs that are in the following provisioning states: Defined, Deployed, Failed, or Discovered. For more information about the provisioning states, see [Circuit or VC States, on page 520](#).



### Note

You cannot change the UNI or endpoint selections. If you want a different device to be an endpoint, you must delete the circuit/VC and create a new one.

For E-LAN and E-TREE EVCs, you can add or delete endpoints (sites).

To modify a circuit/VC:

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.  
The network topology window opens.
- Step 2** From the toolbar, click **Device Groups** and then select the required group.
- Step 3** Click the **Circuits/VCs** tab and then click the radio button for the circuit or VC you want to modify.
- Step 4** From the **Circuits/VCs** pane toolbar, click the pencil (**Modify**) icon.  
The Provisioning Wizard opens and displays information for the selected circuit or VC.
- Step 5** Edit the circuit or VC as required, and then redeploy it. See [Provision EVCs in a Carrier Ethernet Network, on page 436](#) and [Provision Circuits in an Optical/DWDM Network, on page 447](#).
- 

## Activate a Circuit (Optical)

You can activate an optical circuit to determine if the traffic is passing through it. You can activate circuits that are discovered and deployed in the network. Also, the admin status of the circuit must be Down.

- 
- Step 1** From the left side bar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click the **Device Groups** button and select the device group within which the required circuit/VC was created.
- Step 3** In the **Circuits/VCs** tab, locate the optical circuit that you want to activate and click the information icon to access its Circuit/VC 360 view.
- Step 4** Choose **Actions > Activate** to enable the traffic to pass through the optical circuit.
- Note** You can also activate the optical circuit from the Circuit/VC Details window and from the multilayer trace view. See [View Circuits/VCs, on page 88](#) and [Trace and Visualize the Full Route of Circuits/VCs, on page 568](#).
- Step 5** Redeploy the optical circuit.
- 

You can also choose to deactivate the optical circuit to stop the traffic passing through it. Ensure that the circuit is discovered and deployed in the network and the admin status of the circuit is Up. Click **Actions > Deactivate**.

## Restore a Circuit (Optical)

You can restore an optical circuit when it encounters multiple successive failures and reroute the failed circuit over a new route.

You can restore or revert optical circuits that meet the following conditions:

- Circuit's provisioning state is Deployed or Discovered.

- The Restoration attribute for the circuit is set to true.
- The Revert mode for the circuit is set to manual or automatic.

To restore an optical circuit:

- 
- Step 1** From the left side bar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click the **Device Groups** button and select the device group that contains the failed optical circuit.
- Step 3** In the Circuits/VCs tab, locate the failed optical circuit and click the information icon to access its Circuit/VC 360 view.
- Step 4** Choose **Actions > Restoration Actions > Upgrade Restore** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred.

**Note** You can also restore the failed optical circuit from the Circuit/VC Details window and from the multilayer trace view. See [View Circuits/VCs, on page 88](#) and [Trace and Visualize the Full Route of Circuits/VCs, on page 568](#).

---

You can also choose to revert the optical circuit to its original route when the route is recovered from the failure. Click **Actions > Restoration Actions > Manual Revert**.

## Reroute a Circuit (Optical)

You can reroute a circuit to its working path or protected path so that you can perform network maintenance activities without interrupting the service. The reroute operation is available for all WSON circuits that are provisioned or discovered in Cisco EPN Manager .




---

**Note** The reroute operation is not available for circuits that has the restoration status as "Restored" or "Revertible".

---

- 
- Step 1** From the left side bar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click the **Device Groups** button and select the device group within which the required circuit/VC was created.
- Step 3** In the **Circuits/VCs** tab, locate the optical circuit that you want to reroute and click the information icon to access its Circuit/VC 360 view.
- Step 4** Choose **Actions > Reroute Actions > Working Path** or **Protected Path** to reroute the traffic through the working path or protected path defined for the circuit.

**Note** You can also reroute the optical circuit from the multilayer trace view. See [Trace and Visualize the Full Route of Circuits/VCs, on page 568](#).

---

# Compare and Reconcile Provisioned and Discovered Versions of a Circuit/VC



**Note** This functionality is supported for Carrier Ethernet VCs, Circuit Emulation, and Serial services only.

When you provision a circuit/VC using Cisco EPN Manager, the relevant CLI commands are configured on the devices participating in the circuit/VC. After a circuit/VC is provisioned using Cisco EPN Manager, the system discovers the provisioned circuit/VC from the network. In some cases, there might be differences between the provisioned CLI and the discovered CLI, for example, if a configuration change was made on a device after provisioning. Cisco EPN Manager allows you to compare the provisioned and discovered versions of a circuit/VC and generate a reconciliation report showing the differences. Based on the report, you can decide whether to keep the discovered version or revert back to the provisioned version. If you choose to keep the discovered version, the circuit/VC in the Cisco EPN Manager is synched with this version.

The comparison and reconciliation functionality is accessed from the circuit/VC tables.

The functionality is disabled if the circuit/VC discovery state is Missing or the provisioning state is None, In Progress, or Delete Succeeded.

To compare and reconcile a circuit/VC:

- 
- Step 1** Open a table of circuits/VCs, either the full table of all circuits/VCs in the system (**Inventory > Other > Circuits/VCs and Network Interfaces**) or a list of circuits/VCs for a specific device group (**Maps > Network Topology > Circuits/VCs tab > Circuits/VCs link**).
  - Step 2** In the circuits/VCs table, locate and select the required circuit/VC.
  - Step 3** Choose **Actions > Reconciliation Report**.

A comparison report is displayed, showing the differences in provisioned and discovered attributes on specific devices in the circuit/VC. If there are no differences between the provisioned and discovered attributes, "No data available" is displayed in the report.
  - Step 4** After you have reviewed the report, you can choose to save the discovered version to the database as the current version of the circuit/VC or to revert back to the provisioned version. At the top of the page, select the Provisioned or the Discovered radio button and click **Reconcile**.

If you chose Provisioned, the circuit/VC will be redeployed and the attribute values of the original provisioned circuit/VC will be configured on the devices. If you chose Discovered, the discovered circuit/VC will be stored in the database and this version will replace the original provisioned version. The provisioning status will indicate whether or not the reconcile action was successful.
  - Step 5** If the system requires your input in order to complete the reconciliation, the Provisioning Wizard is launched. Fill in the required information and redeploy the circuit/VC.
-

## Initiate a Protection Switch Action on a Circuit (Optical)

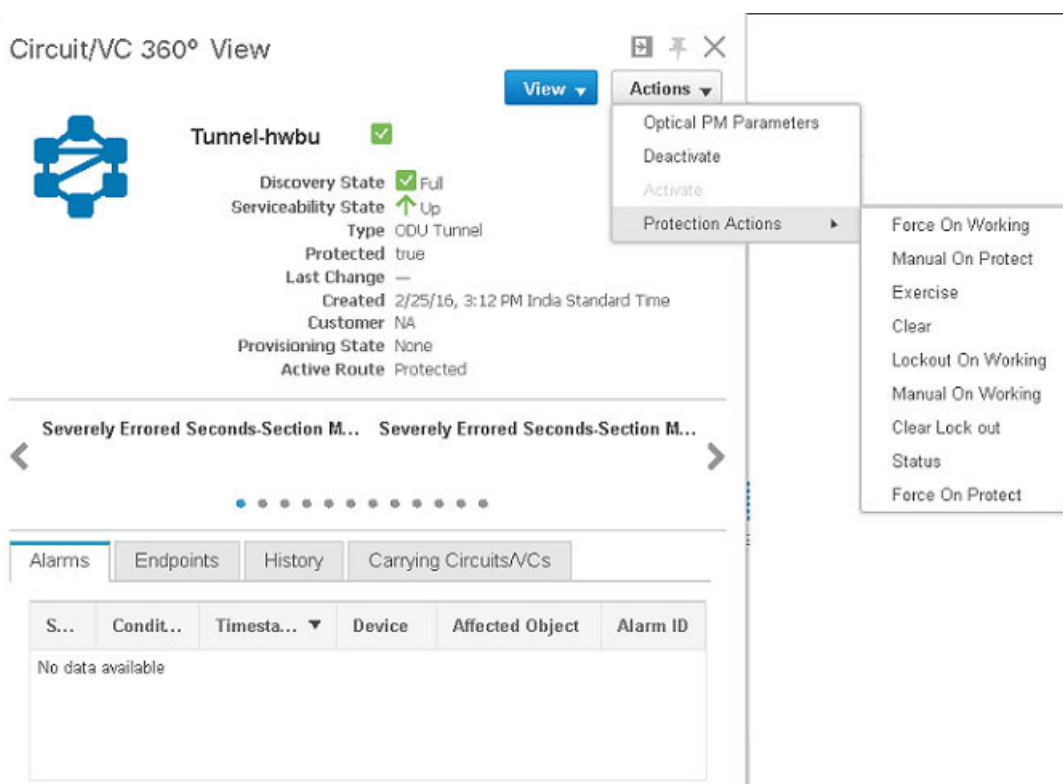
You can initiate a protection switch action on an optical circuit to switch over the traffic from one path to another path. For example, the traffic in an optical circuit is flowing through a working path and the working path is damaged. You can initiate a protection switch action on this circuit to switch over the traffic from the working path to the protected path.



**Note** You can initiate protection switch actions only on optical circuits in which the 1+1 or 1+1+R protection type is enabled. For more information about the protection types, see [Circuit Section Reference for OTN Circuit Types, on page 461](#).

To initiate a protection switch action:

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
  - Step 2** Click **Device Groups**, and then select the location in which the required circuit/VC was created.
  - Step 3** Close the **Device Groups** popup window.
  - Step 4** In the **Network Topology** window, click **Circuits/VCs**.
  - Step 5** On the **Circuits/VCs** tab, locate the required circuit/VC and click the *i* icon next to the circuit/VC name. The Circuit/VC 360 view appears in a separate popup window.
  - Step 6** Choose **Actions > Protection Actions**, and then choose the required protection switch action.



The following table provides a detailed description of each of the protection switch actions.

Protection Switch Action	Description	Applicable when:
Force On Working	Configures the working path to carry traffic over the network.	The current state of the protection switch action is 'Manual On Protect' or 'Manual On Working'.
Manual On Protect	Switches the traffic manually from the working to the protected path.	There is no protection switch action initiated on the circuit.
Clear	Clears the protection switch state on the circuit.	The current state of the protection switch action is not 'Lockout On Working'.
Exercise	Checks if an ODU subcontroller is ready for a protection switch.	There is no protection switch action initiated on the circuit.
Manual On Working	Switches the traffic manually from the protected path to the working path.	There is no protection switch action initiated on the circuit.
Lockout On Working	Configures an ODUk subcontroller as a locked out resource in the ODU subcontroller group. Locks the circuit so that its traffic cannot be switched to the working path.	The current state of the protection switch action is not 'Lockout On Working'.

Clear Lock out	Clears the 'Lockout On Working' switch state for the circuit.	The current state of the protection switch action is 'Lockout On Working'.
Status	Displays the details of ODU subcontroller group and the protection switch state specified in the AID.	Available for all protected optical circuits.
Force On Protect	Configures the protected path to carry traffic over the network.	The current state of the protection switch action is 'Manual On Protect' or 'Manual On Working'.

## Delete a Circuit/VC

You can choose to either delete or force delete a circuit/VC.

You can delete circuits/VCs that are in the following provisioning states: Create/Modify Succeeded or Create/Modify/Delete Failed.

You can force delete circuits/VCs that are in the Delete Failed provisioning state. When you force delete a circuit/VC, it is removed from the Cisco EPN Manager database. The circuit/VC will not appear in the circuit/VC tables.



### Caution

However, the force delete option may not remove the configurations from all the devices participating in the circuit/VC. You may need to manually clean up the devices.



### Note

The force delete option is not available for optical circuits.

To delete or force delete a circuit/VC:

- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.  
The network topology window opens.
- Step 2** From the toolbar, click **Device Groups** and then select the required group.
- Step 3** Click the **Circuits/VCs** tab and then click the radio button for the circuit or VC you want to delete.
- Step 4** From the **Circuits/VCs** pane toolbar, do one of the following:
  - From the X (Delete) icon drop-down list, choose **Force Delete**. A confirmation message is displayed. A corresponding job is created in the Jobs dashboard and you can monitor the progress. Once the job is completed, the circuit/VC is removed from the Cisco EPN Manager database.
  - Click the X (**Delete**) icon. The Provisioning Wizard opens and displays information for the selected circuit or VC.
- Step 5** Click **Next** to go to the **Service Details** page.
- Step 6** In the Deploy area, specify what you expect the delete operation to accomplish:



- Delete the circuit or VC from devices and Cisco EPN Manager —This will remove the configurations from all the devices participating in the circuit or VC and will also remove it from the database. The circuit or VC will not appear in the circuit and VC tables and no history will be available for it.
- Delete the circuit or VC from devices only—The circuit and VC history will remain in the database but all relevant configurations will be removed from the devices participating in the circuit or VC.

**Note** These options are only available in the wizard when deleting an EVC/OVC with "failed" status, for example, "Create failed," Modify failed," and so on.

**Step 7** In the **Deployment Action** field:

- Choose **Preview** to view the configurations that will be deployed to the relevant devices before the actual deployment.
- Choose **Deploy** to deploy the changes without previewing them.

**Step 8** Click **Submit**.

- If you selected **Preview** in the previous step, a Preview Config page is displayed. If you are satisfied with the changes, click **Deploy**.
- If you selected **Deploy** in the previous step, the configurations are deployed to the devices immediately.

A confirmation message is displayed when the deployment is complete.

---

To view the details of configuration, configuration errors, rollback configuration, and rollback configuration errors for each device participating in the circuit/VC, click the *i* icon next to the **Provisioning** column in the Deleted Circuits/VCs tab in the extended tables. The *i* icon is available for all provisioning states, except None. For information about how to access the extended tables, see [View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map, on page 151](#).

## Delete an L3VPN Service

You can delete L3VPN services that were originally created using Cisco EPN Manager . L3VPN services that were only discovered but not created using Cisco EPN Manager cannot be deleted.

To delete an L3VPN service:

---

**Step 1** In the left sidebar, choose **Maps > Network Topology**.

**Step 2** In the Circuits/VCs panel, click the **Circuit/VCs** link to display all services in Cisco EPN Manager .

**Step 3** Select the service that you want to delete. You can type the service's name in the **Name** filter to filter out the required L3VPN service and click the X (**Delete**) icon.

**Step 4** Alternately, from the **Circuits/VCs** pane toolbar, choose the service you want to delete and click the X (**Delete**) icon. The Provisioning Wizard opens and displays information for the selected circuit or VC.

**Step 5** Click the delete icon.

The L3VPN Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN.

**Step 6** Select **Submit** to preview the configuration that is to be pushed on the device.

**Step 7** Review the configuration and click **Deploy** to confirm.

The selected L3VPN service is deleted from the device.

**Note** If the selected L3VPN service uses integrated routing and switching (BVI/virtual interfaces), then deleting the L3VPN service automatically deletes the associated BVI/virtual interface from the device. The BGP and VRF settings associated with the L3VPN service are also deleted.

**Step 8** To verify that the selected L3VPN was deleted from the device, view the complete list of L3VPN services from the Circuits/VCs list.

## Delete an L3VPN Service Endpoint

You can delete L3VPN service endpoints for L3VPN services created using Cisco EPN Manager . Endpoints associated with L3VPN services that are discovered but not created using Cisco EPN Manager cannot be deleted.

To delete an L3VPN service endpoint:

**Step 1** In the left sidebar, choose **Maps > Network Topology**.

**Step 2** In the Circuits/VCs panel, click the **Circuit/VCs** link to display all services in Cisco EPN Manager .

**Step 3** Select the service that you want to delete. You can type the service's name in the **Name** filter to filter out the required L3VPN service.

**Step 4** Click the pencil **Modify** icon.

The L3VPN Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN.

**Step 5** Choose **Delete Endpoint** and click **Next**.

**Step 6** Choose the IP endpoints that must be deassociated from the selected L3VPN service. For single endpoint VRFs, deleting the endpoints turns the VRF ineffective and the VRF then acts as a dangling VRF. To associate newer endpoints with this ineffective VRF, you need to further edit the VRF's attributes.

**Step 7** Click **Next** to preview the configuration that will be pushed to the device.

**Step 8** Review the configuration and click **Deploy** to confirm and deploy your changes to the device.

The selected L3VPN service endpoint is deleted from the device.

## Delete an MPLS TE Service

You can delete MPLS TE services that are in the following provisioning states: Planned, Succeeded, or Failed. For more information about the provisioning states, see [Circuit or VC States, on page 520](#).



**Note** You cannot delete an MPLS TE service if it is being used by a CEM service or a Carrier Ethernet circuit/VC.

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Click **Device Groups**, and then select the location in which the required circuit/VC was created.
- Step 3** Close the **Device Groups** popup window.
- Step 4** In the **Network Topology** window, click **Circuits/VCs**.
- Step 5** In the **Circuits/VCs** tab, click the Circuits/VCs hyperlink located below the list of circuits/VCs.
- Step 6** In the displayed table of circuits/VCs, select the MPLS TE service that you want to delete.
- Step 7** Click the delete icon to open the Provisioning Wizard and display information for the selected MPLS TE service.
- Step 8** From the **Deployment Action** drop-down list, choose one of the following option:
- **Preview**—View the configurations that will be deployed to the relevant devices before the actual deployment.
  - **Deploy**—Deploy the changes without previewing them.
- Step 9** Click **Submit**.
- If you selected Preview in the previous step, Cisco EPN Manager displays a Preview Config page. If you are satisfied with the changes, click **Deploy**.
  - If you selected Deploy in the previous step, Cisco EPN Manager deploys the configurations to the devices immediately.
- 

Cisco EPN Manager displays a confirmation message when the deployment is complete.

## Manage Provisioned Network Interfaces

Cisco EPN Manager provides a table of interfaces that have been provisioned as network interfaces (UNIs or ENNIs) so that you can view details for and manage network interfaces independently of provisioned circuits/VCs. The table provides information about each network interface, including its identifying information, the device it belongs to, the actual interface on the device, and the number of services in which the network interface is currently participating.

You can view:

- The network interfaces in a specific device group (from the Network Topology window).
- All network interfaces managed by Cisco EPN Manager (from the Inventory menu).

You can edit a network interface by clicking the **Edit** button. This launches the wizard where you can make changes to the network interfaces as required. Keep in mind that if the network interface is associated with multiple services, your edit operation will affect all of those services.

You can delete a network interface as long as it is not participating in any circuits.

- 
- Step 1** To view and manage the network interfaces that belong to a specific device group:
- a) In the left sidebar menu, choose **Maps > Topology Maps > Network Topology**.

- b) Click the **Device Groups** button and select the required group.
- c) In the **Circuits/VCs** tab, click the **Network Interfaces** hyperlink (below the table).

**Step 2** To view and manage all network interfaces managed by Cisco EPN Manager , choose **Inventory > Other > Network Interfaces**.

---

## Delete Network Interfaces

From the Network Interfaces table, you can delete a UNI/ENNI if it is not currently participating in any circuits.

To delete a network interface:

---

**Step 1** In the left sidebar, choose **Maps > Topology Maps > Network Topology**.

**Step 2** Click the **Device Groups** button and select the required group.

**Step 3** In the **Circuits/VCs** tab, click the **Network Interfaces** hyperlink to display the Network Interfaces table.

**Step 4** Select the network interface you want to delete and click the **Delete** button. If the network interface is participating in one or more circuits/VCs, the Delete button will be disabled. In the No. of Circuits/VCs column, you can see the number of circuits/VCs in which the network interface is included.

---



## CHAPTER 18

# Monitor and Troubleshoot Circuits/VCs

- [Check Circuits/VCs for Faults, on page 551](#)
- [Identify Which Circuits/VCs are Affected by a Specific Fault, on page 552](#)
- [Get More Information About a Circuit/VC Failure, on page 553](#)
- [Troubleshoot a Service Failure Using OAM Commands, on page 554](#)
- [Use EOAM Templates to Troubleshoot EVCs, on page 558](#)
- [Run a Performance Test on a Circuit/VC, on page 558](#)
- [View Performance Metrics and Reports for Circuits/VCs, on page 566](#)
- [Trace and Visualize the Full Route of Circuits/VCs, on page 568](#)

## Check Circuits/VCs for Faults

Cisco EPN Manager provides several ways to see, at a glance, if there are any problems with circuits/VCs:

- **Circuit list**—The colored icon to the left of each circuit/VC name indicates the primary state of the circuit/VC. If the primary state indicates a problem with the circuit/VC, you can access detailed alarm information for the circuit/VC, as described below.
- **Circuit/VC 360 view**—The Alarms tab in the Circuit/VC 360 view shows all alarms on all devices over which the circuit/VC is configured. Click the information icon next to the circuit/VC name to access the Circuit/VC 360 view.
- **Alarm Table**—The alarm table shows all alarms for all devices, for a specific device group, or for a specific device. Choose **Monitor > Monitoring Tools > Alarms and Events** to access the alarm table. If you have identified an alarm in the Circuit/VC 360 view, you can get more details about the alarm in the alarm table. You can search for the alarm or for the device/link that generated the alarm using the quick filter or the advanced filter. Each alarm in the table can be expanded to show detailed information about the alarm, including which circuits/VCs are affected by the alarm.
- **Circuit/VC Overlay in the Network Topology**—When a circuit/VC is selected in the Circuits/VCs list, it is represented on the network topology as an overlay on top of the existing topology. If the alarm is on a specific device, the alarm badge will appear on the device as usual. If the alarm is on the link between the circuit/VC endpoints, the alarm badge will appear on the link.
- **Multi-layer trace for optical circuits**—See [Trace and Visualize the Full Route of Circuits/VCs, on page 568](#).

# Identify Which Circuits/VCs are Affected by a Specific Fault

To identify which circuits/VCs are affected by a specific fault:

- 
- Step 1** From the left side bar, choose **Monitor > Monitoring Tools > Alarms and Events**.
  - Step 2** In the alarm table, locate the required alarm. You can use the simple or advanced filters to locate the alarm, if necessary.
  - Step 3** Click on the arrow to the left of the row to expand the row and display the alarm details.
  - Step 4** Locate the Impacted Circuits/VCs pane. All circuits/VCs that are affected by the selected alarm are listed in this pane, with basic information for each circuit/VC. You can access the Circuit/VC 360 view to get more details about the circuit/VC by clicking the *i* icon.
  - Step 5** If necessary, you can modify or delete the circuit/VC from the Impacted Circuits/VCs pane by selecting a circuit/VC and clicking the Modify or Delete button. This opens the Provisioning Wizard. See [Modify a Circuit/VC, on page 540](#) and [Delete a Circuit/VC, on page 546](#) for more information.
-

Alarms Events Syslogs Cleared Alarms

Selected 1 / Total 19

Change Status Assign Annotation Delete Show Quick Filter

	Severity	Message	Status	Failure Source	Timestamp	Owner	Categ...	Condition
<input type="checkbox"/>	Major	Device 'ME3800X-PAN-1.cisco.com'. Pseudowire tunnel with Local IP '4.4.4.4', PwId '115', and Remote IP '9.9.9.9' is down	Not Active	ME3800X-PAN-1	March 4, 2015 4:50:33 PM IST		Switches and Hubs	Pseudowire...

**General Information**

Source 10.56.23.27

Acknowledged No

Category Switches and Hubs

Alarm Found At March 4, 2015 4:44:02 PM IST

Alarm Last Updated At March 4, 2015 4:50:33 PM IST

Alarm Detected Through Carrier Ethernet

Severity Major

Previous Severity Cleared

**Messages**

Device 'ME3800X-PAN-1.cisco.com'. Pseudowire tunnel with Local IP '4.4.4.4', PwId '115', and Remote IP '9.9.9.9' is down

**Impacted Circuits/VCS**

Alarms	Name	Type	Date Created	Last Modified	Customer
Major	EvcLink_EthPw...	EVC	March 04, 2015 16:...	March 04, 2015 16:...	Unknown

## Get More Information About a Circuit/VC Failure

Cisco EPN Manager provides information about why the provisioning operation of a circuit/VC has failed so that you can troubleshoot the issues. In the Circuits/VCS table, you can identify problems with a circuit/VC by looking at the Provisioning state and the Serviceability and Discovery states. If there has been an error during the provisioning of a circuit/VC and the circuit/VC could not be created, the Provisioning state will be Create Failed. You can click the *i* icon in the Provisioning column to see the configuration of the devices involved in the failure, as well as details about the specific error(s) that occurred.

For optical circuits, the combination of Serviceability state Down and Discovery state Partial can indicate a problem with the circuit. In this case, you can click the *i* icon in the Serviceability column to see the reason that the Serviceability state is Down.



**Note** Information about a circuit/VC failure can also be accessed from the Circuit/VC 360 view. See [Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 528](#).

To view additional information about a circuit/VC provisioning failure from the Circuits/VCs table:

- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** In the **Network Topology** window, click the **Circuits/VCs** tab, and then click the **Circuits/VCs** hyperlink. A table listing all the circuits is launched in a separate window.
- Step 3** Locate the circuit for which the provisioning operation has failed. The Provisioning state will be **Create Failed**.
- Step 4** Click the *i* icon next to the **Provisioning** column. A popup window is displayed and lists the devices on which the provisioning errors occurred.
- Step 5** Select a device to see its configuration and error details.
- Step 6** Click the *i* icon next to the **Serviceability** column to view the **Serviceability Details** data pop-up window that displays information about why the provisioning operation has failed for the circuit.

**Note** The *i* icon is available only if the serviceability status is down and the discovery status is partial.

For optical circuits, if the Serviceability state is Down and the Discovery state is Partial, click the *i* icon next to the Serviceability column to view the Serviceability Details data pop-up window that displays information about why the circuit's serviceability state is Down. You can also view the Serviceability Details data pop-up window from the Circuit/VC 360 view. For information about how to access the Circuit/VC 360 view, see [Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 528](#).

Alarms Circuits/VCs Network Interfaces Links									
Selected 1 / Total 14									
Primary...	Alarms	Name	Provisioning	Serviceability	Discovery	Type	Customer	Date Created	
	Cleared	prova	Create succee...	Unavailable	Missing	OCHNC	Unknown	June 06, 2016 01:26:10 PM	
	Critical	Mimma-edit-cepm2	None	Admin Down	Full	OCHCC	Unknown	June 01, 2016 10:29:26 AM	
	Critical	TRAIL-MIMMA-FIXATO	None	Admin Down	Full	OCH-Trail	Unknown	June 01, 2016 10:29:26 AM	
	Critical	TEST-OCHNC	None	Admin Down	Full	OCHNC	Unknown	June 01, 2016 10:29:28 AM	
	Minor	WWWWW	None	Admin Down					
	Cleared	QQQQQ	None	Admin Down					
	Cleared	prova	None	Admin D...					
	Cleared	MXP-IS-IMPLICIT	None	Admin Down					
	Cleared	TRAIL-MXP-IS-IMPLICIT	None	Admin Down	Full	OCH-Trail	Unknown	June 06, 2016 01:31:23 PM	
	Cleared	OCHCC_NCS2KE-235-160_2	None	Up	Partial	OCHCC	Unknown	June 06, 2016 01:31:23 PM	
	Cleared	OCHCC_NCS2KE-235-160_1	None	Up	Partial	OCHCC	Unknown	June 06, 2016 01:31:23 PM	
	Cleared	OCHCC_NCS2KE-235-160_6	None	Up	Partial	OCHCC	Unknown	June 06, 2016 01:31:23 PM	

**Serviceability Details**

NO-AVAILABLE-TYP-MATCHING-REQUEST

**Message Details:**  
CPS-1620: Alien wavelength not provisioned on port Unit-4 ADD 14 (AID: PCHAN-4-14-RX)

## Troubleshoot a Service Failure Using OAM Commands

Cisco EPN Manager provides the ping and traceroute features to troubleshoot service failures. You can use OAM commands to access these features and monitor the connectivity and path between two endpoints in a



service. You can then isolate and resolve the failure. The technologies that are supported for the different IOS devices are:

- MPLS LSP, Pseudowire and CFM: Cisco IOS-XE and Cisco IOS-XR
- MPLS Bidirectional TE Flex LSP and VRFs: Cisco IOS-XE

The launch points for the OAM command vary based on:

- Technology type—[Launching from Network Devices Table, on page 555](#) (This launch point for OAM commands is supported only for the **MPLS LSP** technology.)
- Service type—[Launching from Circuit 360, on page 555](#)
- Event type—[Launching from Alarm Browser, on page 556](#)

You can perform ping or traceroute using the OAM commands to troubleshoot a service failure. See [Perform a Ping or Traceroute Using OAM Command, on page 557](#)

## Launching from Network Devices Table

To launch MPLS LSP technology OAM command from Network Devices table:

- 
- Step 1** Choose **Inventory > Device Management > Network Devices**.
- Step 2** In the Network Devices table, select a MPLS enabled device.
- Step 3** Click the >> icon above the Network Devices table and select **OAM Commands**.
- 

## Launching from Circuit 360

If you are launching OAM command from the Service/Circuit 360, the service type is the criteria that determines the technology that is supported. See [Overview of Circuit/VC Discovery and Provisioning, on page 415](#) to know in detail about the different service types.

To launch OAM command from Circuit 360:

- 
- Step 1** Choose **Maps > Topology Maps > Network Topology**.
- Step 2** In the **Network Topology** window, click the **Circuits/VCs** tab and click the *i* icon next to the circuit to view the Circuit 360. Based on the service type of the circuit you selected, the supported technology OAM commands as mentioned in this table are displayed.

Service Type for which you can launch the OAM command:	Technology supported
Carrier Ethernet	<ul style="list-style-type: none"> <li>• MPLS LSP</li> <li>• Pseudowire</li> <li>• CFM</li> </ul>
Circuit Emulation (CEM)	<ul style="list-style-type: none"> <li>• MPLS LSP</li> <li>• Pseudowire</li> <li>• Bidirectional TE (Flex LSP)</li> </ul>

Service Type for which you can launch the OAM command:	Technology supported
L3VPN	<ul style="list-style-type: none"> <li>• MPLS LSP</li> <li>• VRF</li> </ul>
Bidirectional TE Tunnel (Flex LSP)	<ul style="list-style-type: none"> <li>• MPLS LSP</li> <li>• Bidirectional TE (Flex LSP)</li> </ul>

**Step 3** Click **Actions** and select the **Technology OAM** that is displayed for the service type you chose.

## Launching from Alarm Browser

If you are launching OAM command from the alarm browser, the event type is the criteria that determines the technology that is supported.

To launch OAM command from an alarm browser:

**Step 1** Choose **Monitor > Monitoring Tools > Alarms and Events**.

**Step 2** In the Alarms table, select an alarm with an event type listed in the "Event Type for which you can launch the OAM command" column in this table.

Technology supported	Event Type for which you can launch the OAM command:
MPLS Bidirectional TE Tunnel (Flex LSP)	<ul style="list-style-type: none"> <li>• mplsTunnelUp</li> <li>• mplsTunnelDown</li> <li>• mplstunnelReoptimized</li> <li>• ROUTING-MPLS_TE-5-LSP_UPDOWN</li> <li>• MPLS_TE-5-TUN</li> <li>• MPLS_TE-5-LSP</li> </ul>
VRFs in L3VPN	<ul style="list-style-type: none"> <li>• mplsL3VpnVrfUp</li> <li>• mplsL3VpnVrfDown</li> <li>• mplsL3VpnNumVrfRouteMaxThreshCleared</li> <li>• mplsL3VpnVrfNumVrfRouteMaxThreshExceeded</li> <li>• mplsL3VpnVrfRouteMidThreshExceeded</li> </ul>
Pseudowires in Carrier Ethernet and Circuit Emulation	<ul style="list-style-type: none"> <li>• cpwVcDown</li> <li>• cpwVcUp</li> <li>• XCONNECT-5-PW_STATUS Down</li> <li>• L2-L2VPN_PW-3-UPDOWN</li> </ul>
CFM in Carrier Ethernet	<ul style="list-style-type: none"> <li>• E_CFM-3-REMOTE_MEP_DOWN_TIME_OUT</li> <li>• L2-CFM-6-MEP_CHANGE</li> </ul>

**Step 3** Click **Troubleshoot** above the Alarms table and select **OAM Commands**.

## Perform a Ping or Traceroute Using OAM Command

To perform a ping or traceroute using OAM command:

**Step 1** Launch the **TechnologyOAM Command** window. See [Troubleshoot a Service Failure Using OAM Commands, on page 554](#) for the OAM command launch points for the supported technologies.

**Step 2** Based on the launch point, select the required fields as displayed in this table for the selected technology type.

Technology Type	Launched from Alarm Browser	Launched from Service/Circuit 360
Pseudowire	Details are auto-populated	From the <b>Pseudowire Endpoint</b> drop-down list, choose the endpoint participating in the service.
MPLS LSP	From the <b>Destination LDP ID</b> drop-down list, choose the LDP ID of the destination endpoint participating in the service.	From the <b>Source LDP ID</b> and <b>Destination LDP ID</b> drop-down lists, choose the LDP ID of the source and destination endpoints participating in the service.
MPLS Bidirectional TE Tunnel (Flex LSP)	Choose the tunnel's path as <b>Active</b> , <b>Working</b> , or <b>Path-Protect</b> for which you want to perform a ping or traceroute. Cisco EPN Manager performs the ping or traceroute on both directions, that is, from headend to tailend and vice versa.	Choose the tunnel's path as <b>Active</b> , <b>Working</b> , or <b>Path-Protect</b> for which you want to perform a ping or traceroute. Cisco EPN Manager performs the ping or traceroute on both directions, that is, from headend to tailend and vice versa.
VRF in L3VPN	From the <b>End Points</b> drop-down list, choose the endpoint of another VRF that belongs to the same VPN.	From the <b>Source End Points</b> and <b>Destination End Points</b> drop-down lists, choose the source and destination endpoints of another VRF that belongs to the same VPN.
CFM in Carrier Ethernet	From the <b>Destination MEP ID</b> drop-down list, choose the MEP ID of the destination endpoint participating in the service.	From the <b>Source MEP ID</b> and <b>Destination MEP ID</b> drop-down lists, choose the MEP IDs of the source and destination endpoints participating in the service.

**Step 3** Choose **Actions > Ping** to perform a ping, and choose **Actions > Traceroute** to perform a traceroute.

The results of the ping and traceroute commands are displayed in the following formats:



**Note**

- For MPLS bidirectional TE tunnels, the results are displayed for both directions, that is, from headend to tailend and vice versa.
- For Pseudowire, the results are displayed in visual and tabular formats and as raw data.

- **Visual**—The service with the endpoints and its hops is displayed on a map. Hover your mouse cursor over the endpoints to view additional information such as the outgoing and incoming interfaces.




---

**Note** The traceroute command results for all the technologies are displayed in visual format.

---

- **Table Data**—The information such as the outgoing and incoming interfaces, device names, and labels of the endpoints participating in the service are displayed in a tabular format.




---

**Note** Only the traceroute command results are displayed in tabular format.

---

- **Raw Data**—The information about the endpoints participating in the service is displayed as unformatted source data.




---

**Note** Both ping and traceroute command results are displayed as raw data.

---

## Use EOAM Templates to Troubleshoot EVCs

Cisco EPN Manager provides several predefined templates that can be used to monitor the connectivity and performance of virtual connections (VCs) in a Carrier Ethernet network. To use these templates, choose **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI**. See [Perform EOAM Connectivity and Performance Checks, on page 366](#) for more information.

## Run a Performance Test on a Circuit/VC

When you run a performance test, Cisco EPN Manager connects to the network elements to provide real-time data. To get historical information, see [View Performance Metrics and Reports for Circuits/VCs, on page 566](#).

- [Performance Test Based on Y.1564 for EVCs, on page 558](#)
- [Performance Test Based on Y1731 for EVCs, on page 561](#)
- [Performance Test for Optical Circuits, on page 562](#)
- [Performance Test for Circuit Emulation Services, on page 565](#)

## Performance Test Based on Y.1564 for EVCs

CE performance tests verify the correct configuration and performance of CE EVCs at the time of activation. You can also use the CE performance tests to troubleshoot an EVC that is already in operation.

The Y.1564 Ethernet service activation or performance test methodology allows turning up, installing, and troubleshooting Ethernet-based services. Using this test, you can verify the service configuration and

performance from UNI to UNI. This ensures that the SLA will be met according to the bandwidth profile purchased, and the promised class of service.

These tests provide complete validation of Ethernet service-level agreements (SLAs) in a single test. Using a traffic generator performance profile, you can create the traffic based on your requirements. The network performance, such as throughput, loss, and availability, are analyzed using Layer 2 traffic with various bandwidth profiles.



---

**Note** You can only run performance tests on EVCs that are configured on the network and discovered by Cisco EPN Manager .

---

## Supported Devices

The Y.1564 performance test is supported on the following devices running IOS 15.4(S) or IOS XE 3.12S and higher:

- List of devices that can be specified as either source or destination:
  - Cisco ASR 920
  - Cisco ASR 920 24SZIM
  - Cisco ASR 920 24TZM
  - Cisco ASR 920 24SZM
  - Cisco ASR 920 4S ZD
  - Cisco ASR 920 8S Z0A
  - Cisco ASR 920 12 CZA
  - Cisco ASR 920 12 CZD
  - Cisco ASR 920 4S ZA
  - Cisco ASR 920 8S Z0D
  - Cisco ASR 920 12 CZ IM
  - Cisco ASR 901
  - Cisco ASR 901S
  - Cisco ASR 901\_10G
  - Cisco ASR 903 RSP2/RSP3
  - Cisco NCS 4201
  - Cisco NCS 4202
  - Cisco ME 3600X-24CX-M
  - Cisco ME 3600X-24CXE-M
  - Cisco ME1200

- List of devices that can be specified as destination (loopback) only:
  - Cisco ME3800X
  - Cisco NCS 4206
  - Cisco ASR 903 RSP/RSP1

## Running a Y.1564 Performance Test

To run a Y.1564 performance test on an EVC, do the following:

### Before you begin

If you want to run a Y.1564 performance test on an EVC that resides on a ME1200 device, enter the following QoS configuration on both the source and destination interfaces before you run the test:

```
Interface <interface-name>
qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
```

- 
- Step 1** Choose **Maps > Topology Maps > Network Topology** to open the **Network Topology** page.
- Step 2** From the toolbar, click **Device Groups** to open the **Device Groups** pop-up window.
- Step 3** Locate and click the device group that contains the circuit/VC you want to test, then close the pop-up window.
- Step 4** Click the **Circuits/VCs** tab, locate the relevant service, and then click its *i* (**information**) icon to open its **Circuit/VC 360** view.
- Step 5** From the top right corner of the view, choose **Actions > Y.1564 Test** to open the Y.1564 performance test settings page.

**Note** This test can also be initiated from the **Circuit/VC** tab in a device's **Device 360** view and the **Circuits/VCs & Network Interfaces** page. See [View a Device Group's Circuits/VCs, on page 535](#) and [View Circuits/VCs, on page 88](#).

- Step 6** Configure the settings for the performance test:
- In the **Test Mode** field, specify whether this will be a one- or two-way test by clicking the appropriate radio button. Note that in the case of a two-way test, loopback will be created on the service instance of the destination device.
  - In the **End Points** area, choose the source and destination device, interface, and EFP ID from the drop-down lists.
  - In the **Service Configuration Test** area, specify the duration of each iteration, the size of packets to be generated, and the rate at which traffic will be generated.
    - If you choose the **CIR/EIR** radio button, specify values (in kilobits per second) for the Committed Information Rate (CIR) and Excess Information Rate (EIR). The CIR is the long-term average transmission rate, whereas the EIR is the long-term average excess transmission rate.
    - If you select the **Color Aware Test** check-box, specify the Class of Service (CoS) values between 0 to 7 for the **Conform Action** and **Exceed Action**. The CoS values must be set different for **Conform Action** and **Exceed Action** to differentiate and prioritize the traffic. Also, you may specify the values (in kilobytes per second) for

the Committed Burst Size (CBS) and Excess Burst Size (EBS) to define the committed or excess traffic that can be transmitted in bursts at temporary rates above the CIR.

**Note** The **Color Aware Test** check-box will be enabled only for FPGA enabled devices with 10G ports. “Color Aware” is used to describe the mode where the customer is marking each frame as green or yellow, and the network takes this marking into account at the bandwidth profiler and traffic policer.

- If you check the **Step Load CIR** check box, the test will generate traffic at four different levels: 25, 50, 75, and 100% of the CIR value you specify. Note that this option is not available if the CIR is set to a value lower than 8 kbps.
  - If you choose the **Custom Rates** radio button, 1000 kbps is set by default. Change this value, if necessary.
  - If you are running a one-way performance test, you can only specify a custom traffic rate.
- d) In the **Service Acceptance Criteria** area, enter the highest acceptable frame loss ratio value (in percent) in the **FLR** field.
- If you also want to set a frame transfer delay (FTD) and frame delay variation (FDV) value, check the corresponding check box and then enter the appropriate value (in milliseconds).
  - If any of the thresholds you set are exceeded during the performance test, the EVC will be deemed as having failed the test.
- e) (Optional) In the **Frame Settings** area, specify values for the following parameters:
- IP version—IPv4 or IPv6
  - Inner and outer VLAN ID—Identify the source and destination VLAN ID you want to test

**Step 7** Click **Run Test**.

When the test is completed, the results are displayed at the bottom of the Y.1564 performance test settings page.

---

## Performance Test Based on Y1731 for EVCs

The Y.1731 Performance Monitoring (PM) provides a standard ethernet PM function that includes measurement of ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard and interpreted by the Metro Ethernet Forum (MEF) standards group. Using this test, you can verify the delay and loss measurements such as the delay and loss probe status, delay and loss probe availability, two-way delay, two-way jitter, loss forward, and loss backward for your circuit/VC.



---

**Note** This performance test is supported on Cisco IOS and Cisco IOS-XR devices only.

---

### Before you begin

Following are the prerequisites that must be met before you run a performance test based on Y.1731 for a circuit/VC:

- The circuit/VC, along with the participating devices, on which you want to run the performance test, must be operationally up.
- Ensure that the MEP ID matches the domain name for all the devices participating in the circuit/VC.

---

**Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.

**Step 2** Click **Device Groups**, and then select the location that contains the circuit/VC you want to test.

**Step 3** In the **Network Topology** window, click **Circuits/VCs**.

**Step 4** Locate the required circuit/VC, and then click the information icon to access its Circuit/VC 360 view.

**Step 5** Choose **Actions > Y.1731 Test**.

**Note** The performance test can also be initiated from the circuit/VC details window and from the expanded list of circuits/VCs. See [View a Device Group's Circuits/VCs, on page 535](#) and [View Circuits/VCs, on page 88](#).

**Step 6** Choose the required source and destination devices and their corresponding interfaces.

**Step 7** From the CoS drop-down list, choose the priority of the probe. The default value is 0.

**Step 8** Choose the required measurement type. The options are **Delay**, **Loss**, and **Loss & Delay**.

**Note** While delay measurement is done using Delay Measurement Message (DMM) probe, loss measurement is done by Synthetic Loss Measurement Message (SLM) probe. In case of ASR 1K devices, delay measurement using Loss Measurement Message (LLM) probe is only supported.

**Step 9** If required, define the advanced performance test parameters as follows:

- **Probe Length**—Choose the length of the probe in seconds. For example, if the probe length is set to 30 seconds, the statistical data is collected every 30 seconds and displayed in the test results area.
- **Packet Size**—Enter the size (in bytes) of the packets that you want to send for each probe.
- **Burst Interval**—Choose the burst interval in seconds. This defines the time interval between two sets of packets that are sent for a probe.
- **Packet Interval**—Choose the packet interval in milliseconds. This defines the time interval between two packets that are sent for a burst.
- **Packet Count**—Enter the number of packets that will be sent for a burst.

For example, if the burst interval, packet interval, and packet count are set to 30 sec, 1000 ms, and 10 respectively, 10 packets will be sent in the interval of 1000 ms between one packet and the next packet. Once all the 10 packets are sent, there will be an interval of 30 sec after which the next set of 10 packets will be sent.

**Step 10** Click **Run Test**. When the test is completed, the results will be displayed at the bottom of the Performance Test page, under the Test Results area.

---

## Performance Test for Optical Circuits

Cisco EPN Manager performance test for optical circuits is based on the ITU-T recommendations as defined in G.709 and G.798.

Cisco EPN Manager supports the following performance tests for Optical Circuits:



- [Optical Performance Monitoring Parameters, on page 563](#)
- [Run PRBS Test on Circuits \(ODU UNI\), on page 563](#)

## Optical Performance Monitoring Parameters

Optical Performance Monitoring Parameters monitor the quality of optical signals and are used to measure the average optical power transmitted and received between end points in optical circuits. From these measurements, you can derive critical network performance parameters such as channel presence verification, channel wavelength, ASE noise, optical signal power, and optical signal to noise ratio (OSNR) per channel. You can then use these parameters to manage the network reliability and quality of service.

Follow the steps below to view the performance monitoring parameters for an optical circuit:

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Select the device group that contains the circuit/VC you want to test.
- Step 3** In the Circuits/VCS pane on the left, locate the required service and click the *i* icon to access its Circuit/VC 360 view.
- Step 4** Choose **Actions > Optical PM Parameters**.
- Note** The performance test can also be initiated from the circuit/VC details window and from the expanded list of circuits/VCS. See [View a Device Group's Circuits/VCS, on page 535](#) and [View Circuits/VCS, on page 88](#).
- Step 5** Select an optical monitoring type based on which the performance data will be displayed. For more information about the optical monitoring types and the associated performance counters, see [Performance Counters for Optical Monitoring Policies, on page 773](#).
- Step 6** Choose the performance monitoring time interval as 15 minutes or 24 hours to collect the performance data from the device.
- Step 7** Specify the time interval to automatically refresh the performance data.
- Step 8** Click **Auto Refresh**. The performance data for the circuit is displayed as a tabular representation. For the detailed descriptions of the performance data, see [Performance Counters for Optical Monitoring Policies, on page 773](#).
- Based on the time interval specified to refresh the performance data, the newly retrieved data is displayed at the beginning of the table. For example, if the time interval specified is 10 seconds, the performance data is automatically refreshed every 10 seconds and the newly retrieved data is displayed at the beginning of the table. The table displays the last 20 entries of the performance data retrieved.
- 

## Run PRBS Test on Circuits (ODU UNI)

PRBS test is supported for OTN Circuits of type ODU UNI. PRBS bit error count measures the reliability of the link between the endpoints. This test is supported for NCS4K-20T-O-S cards. When PRBS test is run between 2 endpoints (ODU Controller or sub-controller), the source device sends a bit pattern through one or more midpoints (intermediate controller or sub-controller) and the same bit pattern is received by the destination device, the test results can be viewed from both the endpoints. You can also run the PRBS test on a controller, configuring the other endpoint as a loopback, source, or source-sink.

For information on configuring PRBS on an ODU controller, see [Configure PRBS on ODU Controllers, on page 303](#).

To run a PRBS performance test for an optical circuit:

- 
- Step 1** From the left sidebar, choose **Maps > Topology Maps > Network Topology**.
- Step 2** Select the device group that contains the circuit/VC of type ODU UNI you want to test.
- Step 3** In the Circuits/VCS pane on the left, locate the required service and click the *i* icon to access its Circuit/VC 360 view.
- Step 4** Choose **Actions > PRBS Test**.
- Step 5** To assign roles to the endpoints, in the **Endpoint** table, click the endpoint's role and select one of the following options from the drop-down list:
- SOURCE—To set this role to either A or Z side.
  - SINK—To set this role to either A or Z side.
  - SOURCESINK—To set this role either to A side, Z side, or both.
  - INVALID—To disable PRBS on the endpoint.
- Step 6** To assign patterns to the endpoints, in the **Endpoint** table, click the endpoint's pattern and select the desired pattern from the drop-down list.
- Following patterns are supported for NCS4K-20T-O-S cards:
- PRBS 31
  - PRBS 31 Inverted
  - PRBS 11
  - PRBS 11 Inverted
- Step 7** To change the loopback mode, in the Loopbacks table, click the endpoint's or midpoint's loopback mode and select one of the following options from the drop-down:
- NO\_LOOPBACK—For testing without loopback.
  - INTERNAL—For testing within the same network.
  - LINE—For testing across different network.
- Step 8** In the **Test Results** area, select the endpoint from the **Sink Controller** drop-down list.
- Step 9** Click one of the following **Interval** radio button, to set the time interval to collect the data from the device:
- Current (every 10 seconds)—Displays past 15 minutes results every 10 seconds.
  - 15 Minutes—Displays past 15 minutes historic performance data.
  - 1 Day—Displays past 1 day historic performance data.
- Step 10** Click **Go**.
- Step 11** Click **Auto Refresh**. The test result for the endpoints is displayed as a tabular representation which includes bit error count, packets lost and found timestamps and packet lost and found counts.
- Based on the time interval specified to refresh the test, the newly retrieved data is displayed at the beginning of the table. For example, if the time interval specified is 10 seconds, the data is automatically refreshed every 10 seconds and the newly retrieved data is displayed at the beginning of the table.
-

## Performance Test for Circuit Emulation Services

Bit error rate test (BERT) allows you to test cables and diagnose signal problems in the field. This testing mechanism is supported on the Cisco NCS 42xx Series(T1/E1 Ports). This test generates a specific pattern on to the outgoing data stream of a circuit controller and then analyzes the incoming data stream for the same pattern. The bits that do not match the expected pattern are counted as bit errors.

The bit error rate is determined by comparing the erroneous bits received with the total number of bits received. You can view and analyze the total number of error bits transmitted and the total number of bits received on the circuit. You can retrieve error statistics anytime during the test.

The following table lists the test patterns supported in Cisco NCS 42xx series (T1/E1 Ports) devices.

BERT Pattern	Description
0s	Test pattern consisting of all 0's that is used to test line coding.
1s	Test pattern consisting of all 1's that is used to test alternating line volt and repeaters.
2^11	Pseudo-random repeating test pattern that consists of 2,048 bits.
2^15	Pseudo-random repeating test pattern that consists of 32,767 bits.
2^20-O153	Pseudo-random repeating test pattern that consists of 1,048,575 bits.
2^20-QRSS	Pseudo-random QRSS O.151 test pattern that is 1,048,575 bits in length.
2^23	Pseudo-random 0.151 test pattern that is 8,388,607 bits in length.
alt-0-1	Repeating alternating pattern of zeros and ones.

To run a BERT performance test for a CEM circuit:

- 
- Step 1** From the left sidebar, choose **Inventory > Others > Circuits/VCs & Network Interfaces**.
- Step 2** In the **Circuits/VCs** tab, locate the required CEM service and click the *i* icon to access its Circuit/VC 360 view. In the Circuit/VC 360 view, choose **Actions > Performance Test > BERT**.
- Alternatively, you can reach this page through **Maps > Topology Maps > Network Topology** and from the **Circuits/VCs** pane, access the Circuit/VC 360 view of the required CEM circuit.
- Step 3** In the **Test** tab, select the test direction, source and destination.
- For easy understanding, the pictorial representation of the test in the circuit is displayed, once the source and destination are selected.
- Step 4** To refresh the test data automatically for a defined time interval, in the **Settings** area, enter the time interval in minutes.
- Step 5** Select the pattern from the **BERT Pattern** drop-down list.
- Step 6** You can deliberately inject errors in the frame by specifying the value in **Inject Errors** field and then click **Run Test**. The test result is displayed in the **Test Results** area. See [View and Export the Results of the Performance Test on Circuit Emulation Services, on page 566](#)

- Step 7** To terminate the test, in the **Settings** area, click **Stop** and click **Clear Counter** to reset the values in the **Test Results** area.

## View and Export the Results of the Performance Test on Circuit Emulation Services

At a time, BERT performance test can be performed on any number of CEM circuits but only one test can be performed on a single CEM circuit. The results of the BERT performance test on a CEM circuit is displayed in the **Test Results** area.

- At any point in time, the results of last run/currently running BERT performance test on a CEM circuit is displayed in the **Test Results** area in the **Test** tab.
- If the **Auto-refresh** is enabled (ON), then the test results are auto-refreshed at the specified time period.
- In the **Test Results** area:
  - No test results are displayed, when an Unmanaged Endpoint is chosen as destination for a test.
  - Two set of test results are displayed, each for an endpoint, when a Managed Endpoint is chosen as destination.
- Choose **Monitor > Performance Tests > BERTs**. Here, only a single entry for each CEM circuit is available and it shows either the last run/currently running test on that CEM circuit. Select the required CEM circuit to view its test results.
- To view the historical records of BERT performance results for a specific CEM circuit, in the **History** tab, select the required test from the **Test** drop-down list to view the configuration and its result.

You can export the results of a BERT performance test by clicking the Export icon at the top right corner of the **Test** and **History** tabs of the BERT page (from the Circuit/VC 360 view, choose **Actions > Performance Test > BERT**).

You can also export the list of BERT performance tests from the following pages:

- **Select BERT Test** pop-up window (from the BERT page, click the **History** tab, and then click the **Test** drop-down list to open the **Select BERT Test** pop-up window).
- BERT listing page (choose **Monitor > Performance Tests > BERTs**).

## View Performance Metrics and Reports for Circuits/VCs

The Circuit/VC 360 view provides information about the circuit's recent history. Reports, on the other hand, can retrieve all historical data stored in the database. For real-time information, run a performance test (see [Run a Performance Test on a Circuit/VC](#), on page 558).

- [View Performance Graphs in the Circuit/VC 360 View](#), on page 567
- [Use Performance Reports to Monitor and Troubleshoot Circuits/VCs](#), on page 567
- [Use Service Performance Dashboard to Monitor Circuits/VCs](#), on page 567

## View Performance Graphs in the Circuit/VC 360 View

The Circuit/VC 360 view contains graphs showing various aspects of the circuit/VC performance. This view is helpful if you want to see, at-a-glance, if there are any major issues with circuit/VC performance. For more information, see [Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 528](#).

To access the Circuit/VC 360 view:

- 
- Step 1** From the left side bar, choose **Maps > Topology Maps > Network Topology**. The network topology window opens. See [Visualize the Network Topology, on page 149](#) for a description of the Network Topology window and its functionality.
- Step 2** In the Locations pane on the left, select the device group within which the required circuit/VC was created.
- Step 3** In the Circuits/VCS pane, locate the required circuit/VC and click on the *i* icon next to the circuit/VC name. The Circuit/VC 360 view appears in a separate popup window.
- 

## Use Performance Reports to Monitor and Troubleshoot Circuits/VCS

Cisco EPN Manager provides extensive reporting capabilities that enable you to retrieve in-depth performance information for optical circuits and EVCs. The Report Launch Pad provides access to all Cisco EPN Manager reports. From the Report Launch Pad, you can create and save new reports, view current reports, open specific types of reports, schedule a report to run later, and customize the results of a report.

Choose **Reports > Report Launch Pad** in the left navigation pane to access the reports and the reporting functionality.

For information about Carrier Ethernet performance reports, see [Carrier Ethernet Performance Reports, on page 246](#).

For information about Optical performance reports, see [Optical Performance Reports, on page 253](#).

## Use Service Performance Dashboard to Monitor Circuits/VCS

Service Performance dashboard provides a collection of graphical and tabular representation of Performance measurement for the selected circuit/VC over time. This information is available in the form of customized dashlets. The dashboard menu provides access to all the available Cisco EPN Manager dashboards.

From Service Performance Dashboard, you must select a circuit/VC from the Circuits/VCS drop-down list to view the following information (dashlets):

- Average availability of service endpoints over time.
- Incoming and outgoing traffic measured in bits per second, for services over a specified time period.
- Average delay between the service endpoints over time.
- Average packet loss ratio between the service endpoints over time.
- List of services with highest incoming and outgoing traffic.

To launch the dashboard for a specific service from its Circuit/VC 360 view, click **View** and then choose **Dashboard**.

For more information on the Service Performance dashboards and dashlets, see [Service Performance Dashboard Overview, on page 7](#).

For more information on managing dashboards and dashlets, see [Get Started With Cisco EPN Manager](#) , on page 1.

## Trace and Visualize the Full Route of Circuits/VCs

Use the Multilayer Trace view (MLT) to visualize a circuit in a graphical manner. This view displays the complete circuit span and service trace between two endpoints and can be used to trace the connectivity of a circuit by displaying the source node, the destination node, and any intermediate nodes in graphical format.

Note the following:

- Multilayer Trace view is not supported for L3VPN services, Multipoint Carrier Ethernet circuits/VCs, and Serial services.
- You can launch the Multilayer Trace view for optical circuits only when LMP is configured on the A end device and also between devices participating in the optical circuit.
- For MPLS-TE tunnels, physical topology is required for the Multilayer Trace view, meaning that the physical links must have been discovered using one of the supported protocols, for example, CDP or LLDP.

To trace and visualize the full route of a circuit:

- 
- Step 1** From the left side bar, choose **Maps > Topology Maps > Network Topology**.
  - Step 2** Click **Device Groups** and then select the location in which the required circuit/VC was created.
  - Step 3** On the Network Topology page, click **Circuits/VCs**. The list of circuits/VCs associated with the selected device group is displayed.
  - Step 4** Select a circuit/VC for which you want to view the full route. The overlay of the circuit is displayed on the map.
  - Step 5** Use one of the following ways to switch to the Multilayer Trace view:
    - Click the **Multilayer Trace** hyperlink on the notification that appears right below the topology toolbar.

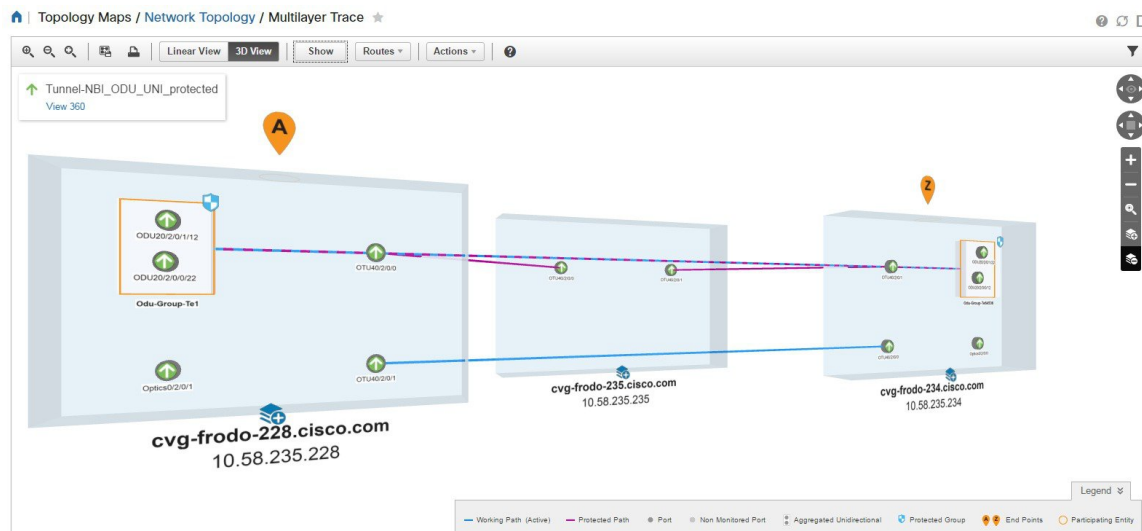
**Note** The **Multilayer Trace** hyperlink appears only if the Multilayer Trace view is supported for the selected circuit/VC and if the primary state of the circuit/VC is not 'Missing' or 'Down'.

- Click the information icon adjacent to the circuit/VC to open the Circuit/VC 360 view, and then click **View>Multilayer Trace**.

The simplified three-dimensional view of the selected circuit/VC is displayed. In the simplified view, only the source and destination endpoints of the participating devices are displayed. You can choose to either expand or collapse the different layers in the circuit/VC. The animation of the route direction between the endpoints is displayed for some circuit types. For more information, see [View Specific Information of a Circuit in a Multilayer Trace View](#), on page 572.

**Note** In the case of a device with a circuit being traversed more than once (more incoming and outgoing connections), the collapse option is disabled in both three-dimensional and linear views.

The following figure shows the simplified view of a circuit/VC with the expand and collapse options.



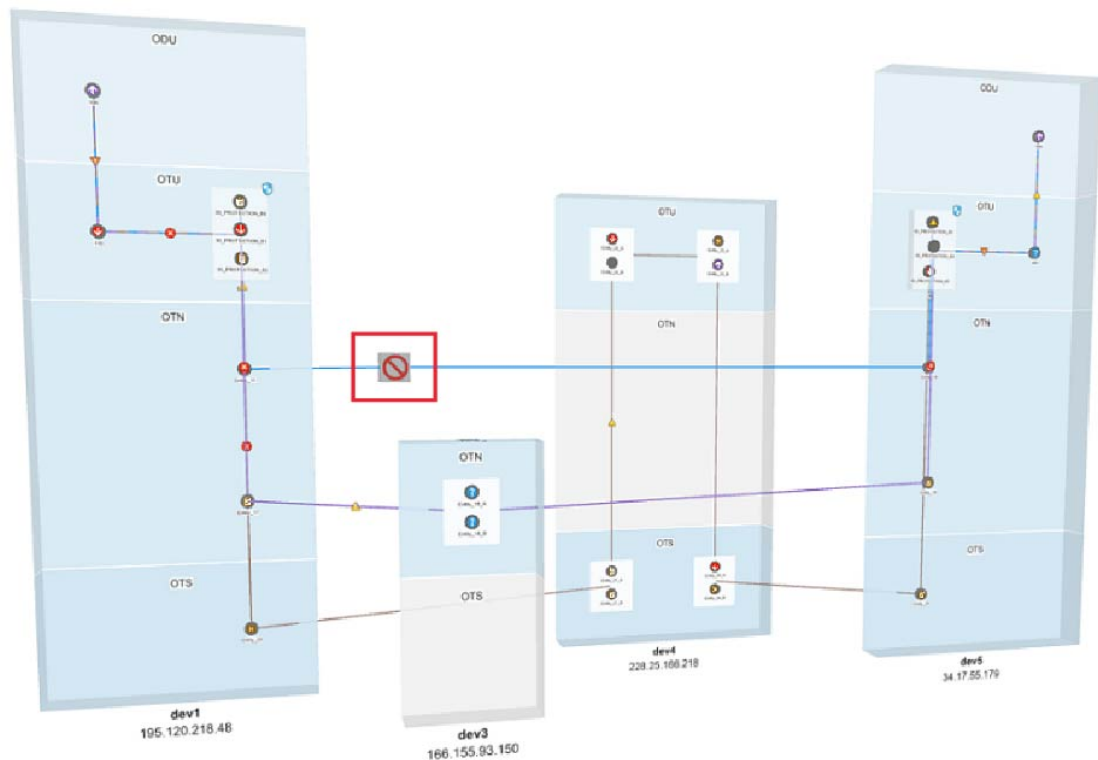
For more information about the details displayed in a three-dimensional view, see [Three-Dimensional View of a Circuit V/C Trace, on page 570](#).

To switch to the linear view, click **Linear View**. For more information about the details displayed in a linear view, see [Linear View of a Circuit/VC Trace, on page 571](#).

The Multilayer Trace view displays a graphical map that:

- Uses high-level span information such as NEs and links to display the circuit trace.
- Displays logical high-level view where the circuit is traced on the map using logical links. For example, OCHCC circuits use OCH trail links for the trace.
- Displays physical high-level view where the circuit is traced on the map using physical links. For example, OCHCC circuits use OTS links for the trace.
- Displays badges on the devices that represent the most severe alarm on the device, irrespective of the selected circuit. The alarm badges within the trace view show the alarms on each entity (for example the link, node, or point).
- Highlights links according to the high-level view that you select.
- Highlights the layers with different shades and displays border lines that delineate the different layers in the circuit. If a layer is not applicable for a device, that layer appears in gray color
- Displays a collapsible legend that lists the different icons and descriptions of each icon displayed in the Multilayer Trace view.
- For optical circuits, indicates whether the devices or links in the circuit have Shared Risk Resource Groups (SRRGs) assigned to them. Click on the SRRG label on the link or device to see a list of all the SRRGs on that link/device. The SRRGs are color-coded based on whether they are the default on the device, assigned, or yet to be assigned. Click on the question mark icon to see the legend.
- For OCHCC circuits, displays the LMP links between the source or destination node and the DWDM controller.

If one or more devices participating in the circuit/VC is not part of your virtual domain, the Multilayer Trace will be partial. Instead of the inaccessible device, you will see an inaccessible device icon in the Multilayer Trace view (as shown in the figure below).



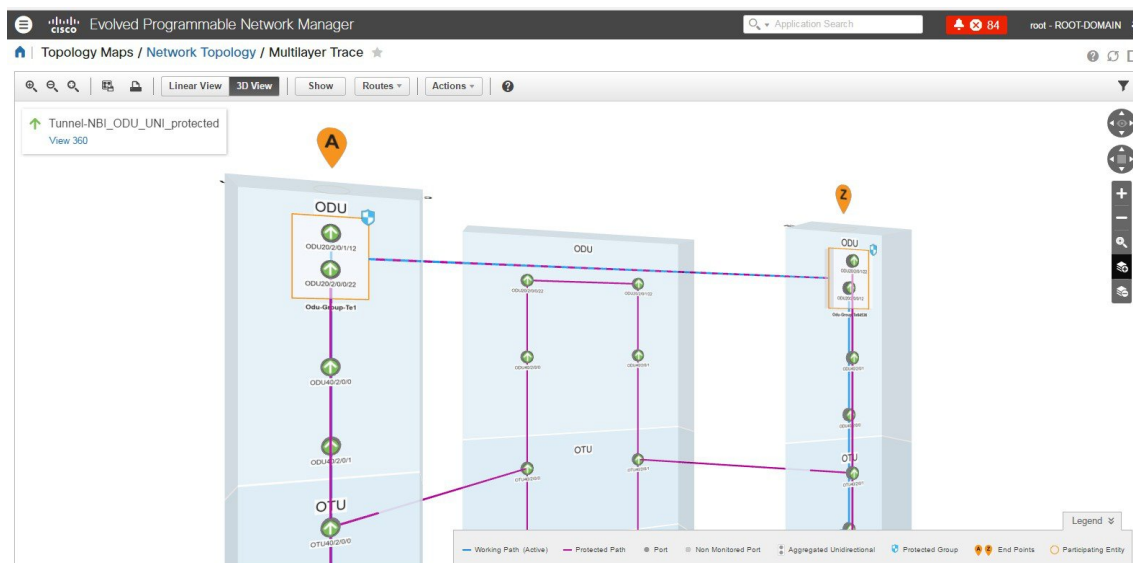
408271

## Three-Dimensional View of a Circuit V/C Trace

This is the default view. It displays a three-dimensional view of the full route of a circuit/VC. For information about how to access this view, see [Trace and Visualize the Full Route of Circuits/VCS, on page 568](#).

This view displays the different paths available for the selected circuit. For example, if an optical circuit has working path, protected path, and restoration path, the paths are color-coded and displayed in this view.

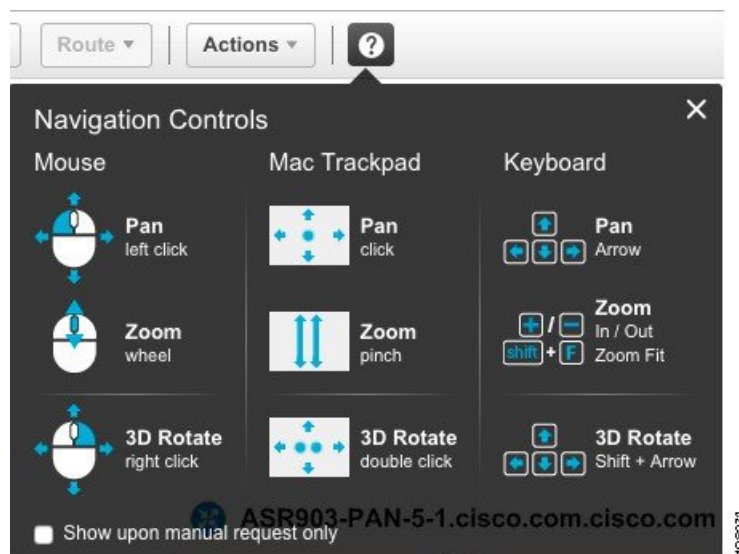




To know about the navigation controls in the three-dimensional view, click the help icon in the tool bar. The Navigation Controls data popup window shows the mouse, MAC Trackpad, and keyboard controls to pan, zoom, and rotate in this view.



**Note** The MAC Trackpad controls are displayed only for MAC users.

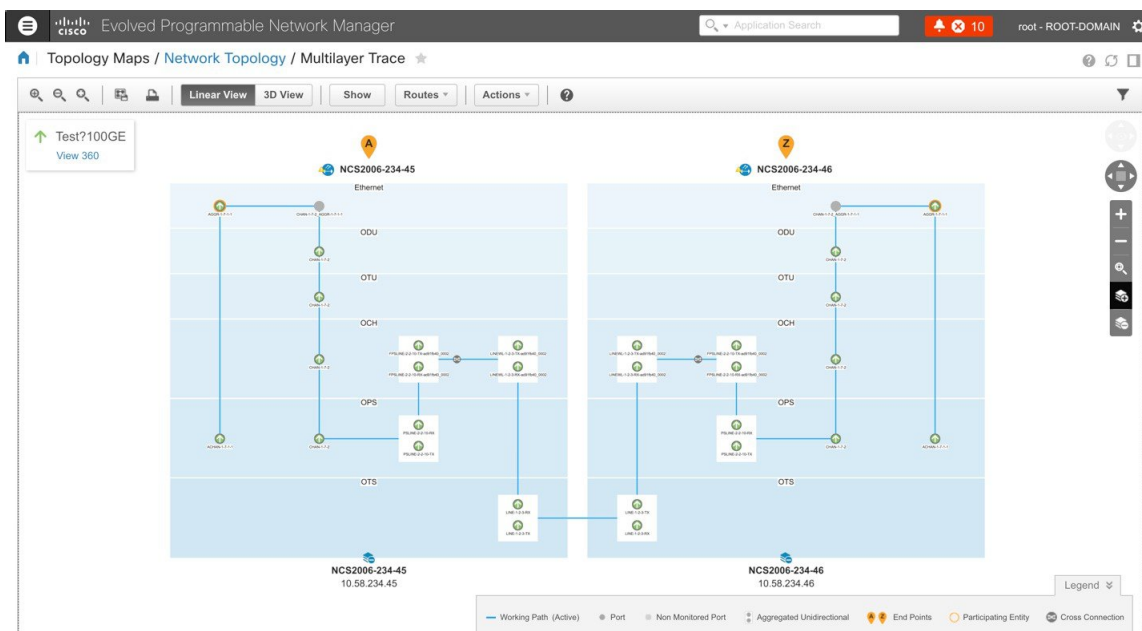


## Linear View of a Circuit/VC Trace

Using the linear view, you can trace and visualize the route of a circuit/VC in a two-dimensional view. For information about how to access this view, see [Trace and Visualize the Full Route of Circuits/VCs, on page 568](#).

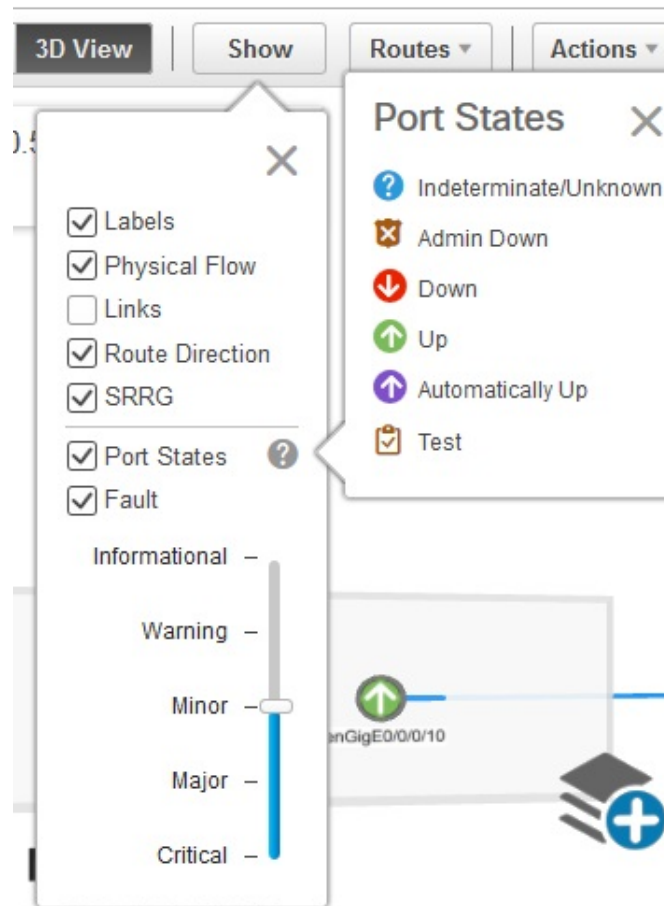
## View Specific Information of a Circuit in a Multilayer Trace View

This view displays only one path of the circuit at a time. Choose **Route**, and then select **Working**, **Protected**, or **Restored** to view the required path in the circuit trace. The path options will vary depending on the type of circuit/VC you selected.



## View Specific Information of a Circuit in a Multilayer Trace View

In the multilayer trace view of a circuit, you can choose what information you want to view by enabling the specific check box from the **Show** menu. You can choose to view the labels, physical flows, links, route directions, SRRG, port states, power levels, span loss, and faults in the circuit. The check boxes vary depending on the type of circuit/VC you selected.



You can view either the alarm status or the primary state of the ports. For a list of the port primary state icons and a description of the states, see [Port or Interface States, on page 78](#).


The **Route Direction** check box to view the animation of the route direction in a circuit, will be enabled by default, only for those circuits which have non-symmetrical paths:

- Unidirectional circuits with path from A to Z. For example, Unidirectional TE Tunnels.
- Bidirectional non-symmetrical circuits with the paths from A to Z and Z to A not being the same. For example, a Carrier Ethernet or a CEM circuit traversing over a unidirectional TE Tunnel.



**Note** The **Route Direction** check box will not appear in the **Show** menu for circuits that have exactly the same path from A to Z and Z to A i.e., bidirectional symmetrical circuits.

By default, the route direction from A to Z end will appear. To view the animation in the opposite direction,

click the  icon. But this icon will be enabled only for those circuits (bidirectional non-symmetrical circuit) that has different A to Z and Z to A paths. For example, a Carrier Ethernet or a CEM circuit traversing over two different unidirectional TE Tunnels. The switch icon does not appear for these circuits:

- Unidirectional circuits with path from A to Z. For example, Unidirectional TE Tunnels.

- Bidirectional symmetrical circuits with the paths from A to Z and Z to A being exactly the same. For example, Bidirectional Core Routed TE Tunnel (or Flex LSP).

When you apply filter to the layers, the **Route Direction** check box gets disabled depending on the chosen layer. Once disabled, it does not get auto-enabled and you have to manually enable the check box to view the route direction animation again.

In case of a partially discovered circuit or a problematic/unsupported circuit configuration, the default route direction from A to Z might not launch. But these circuits may have a potential Z to A direction, which traverses a different path. Click the **Change Endpoints** hyperlink to configure the endpoints to launch the multilayer trace view in the opposite direction.

## Actions You Can Perform from the Multilayer Trace View

You can do the following from the Multilayer Trace view:

- Choose **Show**, and then check the appropriate check boxes to view the labels, physical flows, links, port states, power levels, span loss, and faults in the circuit. For more information, see [View Specific Information of a Circuit in a Multilayer Trace View, on page 572](#).
- Click the **View 360** hyperlink that appears right below the toolbar in the Multilayer Trace to open the Circuit/VC 360 view. See [Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 528](#).
- Click the Port icon on the circuit trace to open the Interface 360 view. See [Get a Quick Look at a Device Interface: Interface 360 View, on page 83](#).
- Click the device name or device IP address that appears at the top of the device to open the Device 360 view. See [Get Basic Device Information: Device 360 View, on page 63](#).
- Click a link in the Multilayer Trace to open the Link 360 view. See [Get a Quick Look at a Specific Link: Link 360 View, on page 160](#).
- Click the Cross Connection icon on the circuit trace to open the Link Details popup window.




---

**Note** The Cross Connection icon appears on the links where internal ports are used by the circuit/VC. The internal ports are not displayed in the Multilayer Trace view.

---

The following figure shows the Link Details popup window that lists the affected internal ports, port status, layer, and power levels. These details are listed for all the affected internal ports in both directions, that is from A side to Z side and vice versa.

Link Details

NCS2KA-235-143:FPLINE-2-6-RX-d96b7920\_029e&FPLINE-2-6-TX-d96b7920\_029e - NCS2KA-235-143:LINEWL-1-2-3-RX-d96b7920\_029e&LINEWL-1-2-3-TX-d96b7920\_029e

Name FPLINE-2-6-RX-d96b7920\_029e&FPLINE-2-6-TX-d96b7920\_029e&LINEWL-1-2-3-RX-d96b7920\_029e&LINEWL-1-2-3-TX-d96b7920\_029e

Type Cross Connection

A Side NCS2KA-235-143:FPLINE-2-6-RX-d96b7920\_029e&FPLINE-2-6-TX-d96b7920\_029e

Z Side NCS2KA-235-143:LINEWL-1-2-3-RX-d96b7920\_029e&LINEWL-1-2-3-TX-d96b7920\_029e

A - Z

Port State/Fault	Port Name	Layer	Power Level
Up	PLINE-1-4-TX	OPS	
Up	LINEWL-1-4-4-RX-d96b7920_029e	OCH	Rx -43.2
Up	LINE-1-4-4-RX	OPS	Rx -6.7
Up	LINEWL-1-4-18-TX-d96b7920_029e	OCH	Tx -45.1
Up	LINE-1-4-18-TX	OPS	Tx -15.2

Z - A

Port State/Fault	Port Name	Layer	Power Level
Up	LINEWL-1-3-1-RX-d96b7920_029e	OCH	
Up	LINE-1-3-1-RX	OPS	Rx -50
Up	LINEWL-1-3-3-TX-d96b7920_029e	OCH	
Up	LINE-1-3-3-TX	OPS	Tx -50
Up	LINEWL-1-4-18-RX-d96b7920_029e	OCH	Rx -43.5

- Choose **Actions** > **Y.1564 Test** to test the performance of the CE circuit/VC end to end. See [Running a Y.1564 Performance Test](#), on page 560.
- Choose **Actions** > **BER Test** to test the performance of the Circuit Emulation Services. See [Performance Test for Circuit Emulation Services](#), on page 565.
- Choose **Actions** > **Optical PM Parameters** to view the realtime performance monitoring data of the optical circuit/VC. See [Optical Performance Monitoring Parameters](#), on page 563.
- Choose **Actions** > **PRBS Test** to test the performance of the optical circuit/VC end to end. See [Run PRBS Test on Circuits \(ODU UNI\)](#), on page 563.
- Choose **Actions** > **Service Details** to view further details about the circuit. See [Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window](#), on page 532.
- Choose **Actions** > **Restoration Actions** > **Upgrade Restore** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred. See [Restore a Circuit \(Optical\)](#), on page 541.
- Choose **Actions** > **Restoration Actions** > **Manual Revert** to revert the optical circuit to its original route when the route is recovered from the failure. See [Restore a Circuit \(Optical\)](#), on page 541.
- Choose **Actions** > **Reroute Actions** > **Working Path** or **Protected Path** to reroute the traffic through the working path or protected path defined for the circuit. See [Reroute a Circuit \(Optical\)](#), on page 542.
- Choose **Actions** > **Activate** to allow the traffic to pass through the optical circuit. See [Activate a Circuit \(Optical\)](#), on page 541.
- Choose **Actions** > **Deactivate** to stop the traffic passing through the optical circuit. See [Activate a Circuit \(Optical\)](#), on page 541.
- Choose **Actions** > **Protection Actions**, and then choose the required protection switch action to switch over the traffic from one path to another path in a protected optical circuit. See [Initiate a Protection Switch Action on a Circuit \(Optical\)](#), on page 544
- Click the filter icon in the Multilayer Trace view toolbar to view the various layers in the circuit. Choose the layers that you want to be displayed.





## PART VII

# Administer the Cisco EPN Manager System

- [Set Up the Cisco EPN Manager Server, on page 579](#)
- [Licenses and Software Updates, on page 585](#)
- [Cisco EPN Manager Security, on page 599](#)
- [Backup and Restore, on page 613](#)
- [Server Health and Configuration, on page 631](#)
- [Data Collection and Purging, on page 655](#)
- [User Permissions and Device Access, on page 667](#)
- [Fault Management Administration Tasks, on page 705](#)
- [Audits and Logs, on page 717](#)
- [Configure High Availability, on page 723](#)







## CHAPTER 19

# Set Up the Cisco EPN Manager Server

These topics describe the tasks an administrator should perform after Cisco EPN Manager is installed. After these tasks are finished, users can log in and set up their working environment as described in [Get Started With Cisco EPN Manager](#), on page 1.

For information on the various types of Cisco EPN Manager users (for example, CLI and web GUI users), see [How to Transition Between the CLI User Interfaces in Cisco EPN Manager](#), on page 669.



**Note** Be sure to review the important information in [Best Practices: Harden Your Cisco EPN Manager Security](#), on page 743.

- [Server Setup Tasks](#), on page 579
- [User Management Setup Tasks](#), on page 581
- [Fault Management Setup Tasks](#), on page 581
- [Web GUI Setup Tasks \(Admin\)](#), on page 582

## Server Setup Tasks

Task	See
Verify the backup settings	<a href="#">Set Up Automatic Application Backups</a> , on page 623
Install any required product licenses and software updates	<a href="#">Licenses and Software Updates</a> , on page 585
Modify the stored Cisco.com credentials (user name and password) used to log on to Cisco.com and: <ul style="list-style-type: none"><li>• Check for product updates</li><li>• Check for device software image updates</li><li>• Open or review Cisco support cases</li></ul>	<a href="#">Configure Stored Cisco.com Credentials</a> , on page 646

Task	See
For software updates: <ul style="list-style-type: none"> <li>• Enable notifications for product software updates (critical fixes, device support, add-ons)</li> <li>• Specify whether you want credentials stored on Cisco.com when Cisco EPN Manager checks for software updates, and if yes, whether you want the user to be prompted for credentials when checking for updates</li> </ul>	<a href="#">Enable or Disable Notifications About Software Updates, on page 597</a>
Set up HTTPS on the server for secure interactions between the server and browser-based GUI client (you can use HTTP but HTTPS is recommended)	<a href="#">Secure the Connectivity of the Cisco EPN Manager Server, on page 633</a>
Configure high availability	<a href="#">Configure High Availability, on page 723</a>
Adjust data retention and purging	<a href="#">Data Collection and Purging, on page 655</a>
For server-related traps that signal system problems, customize the threshold settings and severities, and forward the traps as SNMP trap notifications to configured receivers	<a href="#">Customize Server Internal SNMP Traps and Forward the Traps, on page 652</a> <a href="#">Forward Alarms and Events as SNMP Trap Notifications, on page 707</a>
Set up NTP (Network Time Protocol) so that time is synchronized between the server and network devices	<a href="#">Set Up NTP on the Server, on page 644</a>
Configure FTP/TFTP on the server for file transfers between the server and network devices	<a href="#">Enable FTP/TFTP/SFTP Service on the Server, on page 646</a>
Configure a proxy for the Cisco EPN Manager server	<a href="#">Set Up the Cisco EPN Manager Proxy Server, on page 645</a>
Configure the email server	<a href="#">Set Up the SMTP E-Mail Server, on page 645</a>
Set global SNMP polling parameters for managed network elements	<a href="#">Configure Global SNMP Settings for Communication with Network Elements, on page 647</a>
Enable the Compliance feature if you plan to use it to identify device configuration deviations	<a href="#">Enable and Disable Compliance Auditing, on page 134</a>
Enable the Service Discovery feature so that Cisco EPN Manager discovers the services that are existing in the network and the services that are provisioned using the Provisioning Wizard.	<a href="#">Enable and Disable Service Discovery, on page 519</a>
Configure product feedback to help Cisco improve its products	<a href="#">Set Up Defaults for Cisco Support Requests, on page 654</a>
Configure product feedback to help Cisco improve its products	<a href="#">Configure Cisco Product Feedback Settings, on page 654</a>

## User Management Setup Tasks

Task	See
Create web GUI users that have administration privileges, and disable the web GUI root account	<a href="#">Create Web GUI Users with Administrator Privileges, on page 678</a> <a href="#">Disable and Enable the Web GUI root User, on page 671</a>
Set up user audits	<a href="#">Audit Configuration Archive and Software Management Changes (Network Audit) , on page 717</a>
Set up user authentication and authorization	<a href="#">Configure External Authentication, on page 691</a> <a href="#">Configure Local Authentication, on page 690</a>
Create user accounts and user groups	<a href="#">Control the Tasks Users Can Perform (User Groups), on page 672</a>
Adjust user security settings (password rules for local authentication, idle time logout setting)	<a href="#">Configure Global Password Policies for Local Authentication, on page 681</a> <a href="#">Configure the Global Timeout for Idle Users, on page 681</a>
Specify which users can approve jobs	<a href="#">Configure Job Approvers and Approve Jobs, on page 680</a>
Create virtual domains to control device access	<a href="#">Create Virtual Domains to Control User Access to Devices, on page 682</a>
Create a message that is displayed when users log in to the GUI client	<a href="#">Create a Login Banner (Login Disclaimer), on page 647</a>

## Fault Management Setup Tasks

Task	See
Forward alarms and events to other receivers in e-mail format	<a href="#">Forward Alarms and Events as Email Notifications (Administrator Procedure), on page 706</a>
Forward alarms and events to other receivers in SNMP trap format	<a href="#">Forward Alarms and Events as SNMP Trap Notifications, on page 707</a>
Configure global settings for alarm and event displays and searches: <ul style="list-style-type: none"> <li>• Hide acknowledged, assigned, and cleared alarms in the Alarms and Events tables</li> <li>• Include acknowledged and assigned alarms in search results</li> <li>• Include device names in alarm messages</li> </ul>	<a href="#">Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms, on page 708</a>

Task	See
Customize the severity for specific events	<a href="#">Change Event Severity Levels, on page 709</a>
Customize the troubleshooting text that is associated with an alarm	<a href="#">Customize the Troubleshooting Text for an Alarm, on page 710</a>
Customize the auto-clear interval for specific alarms	<a href="#">Change Alarm Auto-Clear Intervals, on page 710</a>
Make the text in the alarm <b>Failure Source</b> field more user-friendly	<a href="#">Change Event Severity Levels, on page 709</a>
Customize the behavior of expedited events	<a href="#">Change the Behavior of Expedited Events, on page 711</a>
Control generic event handling	<a href="#">Disable and Enable Generic Trap Processing, on page 712</a>
Control if and how users can create Cisco Support Requests	<a href="#">Set Up Defaults for Cisco Support Requests, on page 654</a>

## Web GUI Setup Tasks (Admin)

Task	See
Disable features or menu items that your deployment does not use	<a href="#">Customize the Web GUI Menus to Disable Cisco EPN Manager Features, on page 582</a>
Set Up the System Monitoring Administration Dashboard	<a href="#">Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard, on page 650</a>

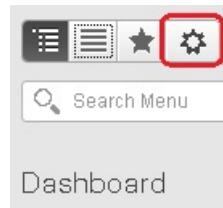
## Customize the Web GUI Menus to Disable Cisco EPN Manager Features

If you belong to the root, Super Users, or Admin user group, you can customize Cisco EPN Manager so that specific menus are no longer displayed in the web GUI. See [View User Groups and Their Members, on page 675](#). This is helpful if your deployment does not use all of the functions in Cisco EPN Manager. When you disable a menu, it is no longer displayed in the web GUI for any users, regardless of their user role.

Complete the following procedure to customize the web GUI by disabling entire features and specific menus. To re-enable the currently disabled features, use the same procedure, but toggle the feature's status to **Enabled** (or click **Enable All**).

---

**Step 1** Click the gear that is displayed above the left sidebar menu.



**Step 2** To disable an entire feature:

1. Locate the feature in the **Feature Navigation Groups** area.
2. In the feature's **Status** column, click the toggle so that it displays **Disabled**.
3. To check which menus will be disabled, scroll through the menus in the **Menu Details** area. All affected menus will be listed as **Disabled**.

**Step 3** To disable specific menus:

1. Locate the menu in the **Menu Details** area.
2. In the menu's **Status** column, click the toggle so that it displays **Disabled**. If you disable a menu that has sub-menus, the sub-menus are also disabled. For example:
  - If you disable **Group Management**, Cisco EPN Manager will disable all of the **Group Management** sub-menus: **Network Device Groups**, **Compute Device Groups**, and **Port Groups**.
  - If you disable only the **Compute Device Groups** sub-menu, Cisco EPN Manager will still display the **Network Device Groups** and **Port Groups** sub-menus under Group Management.
3. To check which menus will be disabled, scroll through the menus in the **Menu Details** area.

**Step 4** Click **Save**, then log out of the web GUI.

**Step 5** Log back into the web GUI and validate your changes.

---





## CHAPTER 20

# Licenses and Software Updates

- [View and Manage Licenses, on page 585](#)
- [Manage Software Updates, on page 596](#)

## View and Manage Licenses

Licenses determine the features you can use and the type and number of devices that Cisco EPN Manager can manage. When you connect to Cisco EPN Manager (without logging in), the login page displays a banner that identifies the type of license the server is running (see [Types of Cisco EPN Manager Licenses, on page 585](#)). If Cisco EPN Manager is configured to use single sign-on (SSO), check the license type by viewing the banner contents.

Cisco EPN Manager supports Cisco Smart Licensing and traditional licensing. If you are currently using traditional licensing, Cisco recommends that you convert to Smart Licensing. For information on the differences between the two types of licensing, refer to the Cisco Smart Licensing Overview on [Cisco.com](http://cisco.com).

You can upgrade Cisco EPN Manager to a new version using one of the following licensing methods:

- Cisco Smart Licensing - In this method, you must register the new instance of the Cisco EPN Manager with the Cisco Smart Software Manager. See [Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 589](#).
- Traditional Licensing - In this method, the files are copied from the previous version of the Cisco EPN Manager to the upgraded version. However, you must purchase the Base license for the upgraded version. To purchase a new traditional license, go to <http://cisco.com/go/license>.

How to use Cisco Smart Licensing and traditional licensing is explained in the following topics:

- [Use Cisco Smart Licensing, on page 586](#)
- [Use Traditional Licensing, on page 593](#)

## Types of Cisco EPN Manager Licenses

The following topics describe the feature- and time-based licenses supported by Cisco EPN Manager .

### Base License

A base license enables all applications and all device drivers (without device count restrictions) on the server. It is displayed in the web GUI as **Base License**.

## Device Right-to-Manage (RTM) License

Device RTM licenses allow the server to manage a specific number of devices of a specific device type. For RTM licenses, the device count is displayed next to the device type. These licenses come in two flavors:

- Extended RTM licenses for core, edge, aggregation, and access network devices. These licenses enable end-to-end network management: device lifecycle management, network provisioning, and network assurance.
- Foundation RTM licenses for service provider Wi-Fi networks that have Wi-Fi access points, WAN routers, core switches, and data center switches. Along with device lifecycle management, these licenses enable assurance visibility and troubleshooting capabilities.

Devices that are configured as satellites (for example, Cisco ASR 903 with a Cisco ASR 9000v host) are counted as independent devices.

Cisco EPN Manager will also discover third party network devices using its Open License "best effort" detection process. The collected information is displayed in the web GUI, but results can vary widely (depending entirely on the responses Cisco EPN Manager receives from the devices). You do not have to purchase any licenses to enable this mechanism.

RTM licenses are displayed in the GUI as follows:

- For Cisco devices—Device model, such as **NCS 2002** or **ASR 9001**.
- For third party devices—**Open License**.

## SBY License for High Availability

The Standby (SBY) license allows the setup of high availability deployments. In a high availability deployment, all the device and feature licenses must be installed on the primary server. No licenses are required on the secondary server.

## NBI License

The NBI license enables all MTOSI- and RESTCONF-related APIs and administrative features on the server. If the NBI license is time-based, the remaining time is listed next to the license. This license is displayed in the GUI as **NBI**.

## Time-Based, Lab, and Permanent Licenses

Most licenses can be purchased as a lab license or time-based license:

- Lab—For lab or staging environments.
- Time-Based (Evaluation)—For a 90-day trial period (the product is disabled when the trial period expires). If you purchase a time-based license, the days remaining are listed next to the license name.

These licenses can be converted to Permanent licenses.

## Use Cisco Smart Licensing

Cisco recommends that you use the simple and efficient Cisco Smart Licensing mechanism to manage your licenses. A comparison of Smart and traditional licensing is provided in the Cisco Smart Licensing Overview on [Cisco.com](https://www.cisco.com). After enabling Smart Licensing in Cisco EPN Manager, you must register Cisco EPN Manager



with the Cisco Smart Software Manager (CSSM) on Cisco.com. After you are registered, all Cisco EPN Manager license types will be available to you from the Cisco EPN Manager web GUI.

If you are currently using traditional licensing, you can convert your existing Cisco EPN Manager licenses to Smart entitlements at any time, as described in [Convert Traditional Licenses to Smart Entitlements](#), on page 590.

The following topics explain how to set up and manage Cisco EPN Manager licenses using Cisco Smart Licensing.

- [Set Up Cisco Smart Licensing in Cisco EPN Manager](#) , on page 587
- [Choose Cisco EPN Manager Licenses Using Smart Licensing](#), on page 590
- [Configure License Thresholds for the Smart License Dashboard](#), on page 591
- [Check Cisco EPN Manager License Usage](#), on page 591
- [Disable Smart Licensing](#), on page 591
- [Reference: Smart Product Registration and License Authorization Statuses](#), on page 592

## Set Up Cisco Smart Licensing in Cisco EPN Manager

Follow these steps to set up Cisco Smart Licensing so you can use it to manage your licenses. If you are currently using traditional licensing, use these same procedures to use Cisco Smart Licensing and, when convenient, convert your existing Cisco EPN Manager licenses as described in [Convert Traditional Licenses to Smart Entitlements](#), on page 590.

	Step	See:
1.	Create a Smart Account with Cisco Systems.	Go to <a href="#">Smart Account Request</a> and follow the instructions on the web site.
2.	Set up communication between Cisco EPN Manager and the CSSM on Cisco.com.	<a href="#">Set Up the Transport Mode Between Cisco EPN Manager and Cisco Smart Software Manager</a> , on page 587
3.	Enable Smart Licensing in Cisco EPN Manager .	<a href="#">Enable Smart Licensing in Cisco EPN Manager</a> , on page 588
4.	Register Cisco EPN Manager with the CSSM on Cisco.com by obtaining a token from the CSSM and entering it in the Cisco EPN Manager web GUI.	<a href="#">Register Cisco EPN Manager with the Cisco Smart Software Manager</a> , on page 589
5.	Choose the licenses you want to use in Cisco EPN Manager .	<a href="#">Choose Cisco EPN Manager Licenses Using Smart Licensing</a> , on page 590
6.	Set up the Smart License Dashboard so you can monitor your licensing usage.	<a href="#">Configure License Thresholds for the Smart License Dashboard</a> , on page 591

### Set Up the Transport Mode Between Cisco EPN Manager and Cisco Smart Software Manager

**Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Account Settings**.

**Step 2** Click the **Smart Licensing Transport** tab and select a communication mode:

- **Direct mode**—Sends license information directly to the cloud. This is the default. You cannot edit this URL. Click **Test Connectivity** to check the connection status.
- **Transport Gateway**—Uses either a Cisco Smart Call Home transport gateway or a Cisco Smart Licensing Software satellite (which is installed at customer premises and provides a subset of CCSM functionality) for communication. (See [Cisco.com](#) for more details.) Enter the appropriate URL in the **Enter URL** field. Click **Test Connectivity** to check the connection status.
- **HTTP/HTTPS Proxy**—Uses either an HTTP or HTTPS proxy for communication between Cisco EPN Manager and the cloud. To enable this option, you must first configure the proxy settings. Click **HTTP/HTTPS Proxy** hyperlink or click the **Proxy** tab to add or edit the proxy settings. See [Set Up the Cisco EPN Manager Proxy Server](#), on page 645.

**Step 3** Click **Save** to save the transport settings.

**Step 4** To revert to the default values, click **Reset**, and then click **Save**.

#### What to do next

If you have not already done so, enable Smart Licensing. See [Enable Smart Licensing in Cisco EPN Manager](#), on page 588.

### Enable Smart Licensing in Cisco EPN Manager

#### Before you begin

Make sure you have set up the transport mode. See [Set Up the Transport Mode Between Cisco EPN Manager and Cisco Smart Software Manager](#), on page 587.

**Step 1** Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.

**Step 2** Enable Cisco Smart Licensing in the Cisco EPN Manager web GUI.

- Click the **Licensing Settings** tab.
- In the **Licensing Mode** field, click **Smart Software Licensing** radio button.
- Choose **Evolved Programmable Network Manager** from the Product Name drop-down list.
- Click **Enable Smart Software Licensing**. Cisco EPN Manager may display a dialog box indicating that when you complete this procedure, you must restart the web GUI before you can proceed with the configuration step.
- Click **OK** in the dialog box.
- If necessary, log out of the web GUI and then log back in.

#### What to do next

Do one of the following:

- If you have not yet registered Cisco EPN Manager with the CSSM on Cisco.com, Cisco EPN Manager will run in evaluation mode (which has a limit of 90 days). Register the product as described in [Register Cisco EPN Manager with the Cisco Smart Software Manager](#), on page 589.
- If you have registered Cisco EPN Manager with the CSSM, select the licenses you want to use. See [Choose Cisco EPN Manager Licenses Using Smart Licensing](#), on page 590.

## Register Cisco EPN Manager with the Cisco Smart Software Manager

To register Cisco EPN Manager with the CSSM, you must obtain a token from the CSSM and enter it into the Cisco EPN Manager web GUI. This is a one-time requirement. If for any reason you have to re-register your product instance, you can do that by following this procedure.



**Note** Refer to the [Cisco Smart Software Manager User Guide](#) for information on how to use the CSSM and the other actions that you can perform from this application—for example, renewing license registration and license authorization, unregistering the product from Cisco Smart Licensing, and so forth.

### Before you begin

If your organization does not have a Smart Account, go to [software.cisco.com](https://software.cisco.com), choose **Request a Smart Account** in the **Administration** area, and follow the instructions to create an account.

- 
- Step 1** Go to the Cisco Software Central web site ([software.cisco.com](https://software.cisco.com)).
- Step 2** Obtain your tokens. If you already have tokens (for example, you converted traditional licensing PAKs to Smart entitlements), proceed to the next step.
- If you are re-registering your product instance, your token will be listed in the CSSM user interface. If your token is no longer valid, you can obtain a new token using this procedure.
1. On Cisco Software Central, choose **License > Smart Software Licensing**.
  2. Select the appropriate virtual account.
  3. Click the **General** tab, then click **New Token**.
  4. Follow the instructions to provide a name, duration, and export compliance applicability before accepting the terms and responsibilities.
  5. Click **Create Token**.
  6. Copy the Token ID to your clipboard and proceed to the next step.
- Step 3** Enter the Token ID into the Cisco EPN Manager web GUI to register the product instance.
1. Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.
  2. Click the **Licensing Settings** tab, then paste your token into the **Registration Token** field.
  3. Click **Register**.
- Step 4** Log out of the Cisco EPN Manager web GUI, then log back in.
- 

### What to do next

Choose the licenses you want to use. See [Choose Cisco EPN Manager Licenses Using Smart Licensing, on page 590](#).

## Choose Cisco EPN Manager Licenses Using Smart Licensing

After you have registered Cisco EPN Manager with the CSSM, all Cisco EPN Manager license types will be listed in the Cisco EPN Manager web GUI, and you can choose the ones you want to use.

---

### Step 1 If this is the first time you are choosing Smart licenses:

- a) Choose **Administration > Licenses and Software Updates > Licenses**.

After a few moments, Cisco EPN Manager displays a dialog box informing you that you cannot access the page because you are not using traditional licensing. This is normal.

- b) In the dialog box, click **Smart License Settings**.
- c) Click the **Licensing Settings** tab.

### Step 2 If you are already using Smart Licensing:

- a) Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.
- b) Click the **Licensing Settings** tab.

### Step 3 Under Smart License Usage, click **Choose Licenses**.

### Step 4 Select licenses from the Available Licenses dialog box, then click **Save**. Cisco EPN Manager immediately begins consuming the licenses.

---

#### What to do next

Configure the Smart License Dashboard thresholds for the new licenses. See [Configure License Thresholds for the Smart License Dashboard, on page 591](#).

## Convert Traditional Licenses to Smart Entitlements

If you have been managing Cisco EPN Manager licenses using traditional licensing, you can enable and configure Smart Licensing by following the setup tasks in [Set Up Cisco Smart Licensing in Cisco EPN Manager, on page 587](#). When convenient, convert your existing traditional licenses to Smart entitlements described in this procedure. You will have to enter your Product Activation Key (PAK) numbers in the License Registration Portal on the Cisco Software Central site.

#### Before you begin

- You must have a Cisco.com account to access Cisco Software Central. If you do not have an account, go to the [Cisco.com registration page](#).
  - Make sure you have your existing traditional licensing PAK numbers.
- 

### Step 1 On Cisco Software Central, choose **License > Traditional Licensing**.

### Step 2 Click **Continue to Product License Registration** to open the License Registration Portal.

### Step 3 In the field under **Get New Licenses**, enter your PAK numbers. If you are entering multiple PAKs, separate them with a comma. You can enter a maximum of 10 PAKs.

- Step 4** Under the **PAKs/Tokens** tab, select the PAKs you want to convert to Smart entitlements, then choose **Actions > Convert to Smart Entitlements**.

## Configure License Thresholds for the Smart License Dashboard

To efficiently manage your licenses, configure the Smart License Dashboard to indicate when Cisco EPN Manager is approaching the point where its licenses will be depleted. The settings you configure here are system-wide .

- Step 1** Choose **Administration > Licenses and Software Updates > Smart Software Licensing**, then click the **License Dashboard Settings** tab.
- Step 2** Make a selection from the **License Type** drop-down list.
- Step 3** Enter a value in the **Threshold Value** field.
- Step 4** Click **Save**.

The threshold value is displayed as a straight line in the graphical representation of the **License Summary** and the **Device Distribution for License** dashlets.

## Check Cisco EPN Manager License Usage

Check current license usage using the Smart Licensing Dashboard. To open the dashboard, choose **Administration > Dashboards > Smart Licensing Dashboard**. For an explanation of the basic license types, see [Types of Cisco EPN Manager Licenses](#), on page 585.

To view these license counts:	Check this part of the dashboard:
For the current date	License Summary Count—Green indicates compliant license counts; red indicates non-compliant license counts.
For a specific week or month	License Summary—Hover over a bar chart to view more details.
For a specific license type	Device Distribution for License—Click one of the license links at the top of the License Summary dashlet. Hover your mouse cursor over the chart to view the details.

## Disable Smart Licensing

- Step 1** Change the license setting in the Cisco EPN Manager web GUI.
- Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.
  - At the bottom of the page, click **Disable Smart Licensing**, then confirm your choice.
- Step 2** Log out of the Cisco EPN Manager web GUI, then log back in.
- Because Cisco EPN Manager is not yet registered to use traditional licensing, when you log back in, all features are disabled. This is normal.
- Step 3** Enable traditional licensing in the Cisco EPN Manager web GUI. (This is done from the Smart License Settings page.)

- a) Choose **Administration > Licenses and Software Updates > Licenses**.

After a few moments, Cisco EPN Manager displays a dialog box informing you that you cannot access the page because you are not using traditional licenses. This is normal.

- b) In the dialog box, click **Smart License Settings**.  
 c) Click the **License Settings** tab.  
 d) For the Licensing Mode, select **Traditional Licensing**.  
 e) Click **Register**.

**Step 4** Log out of Cisco EPN Manager , then log back in.

## Reference: Smart Product Registration and License Authorization Statuses

### Product Registration Status

The License Registration Status reflects whether the product is properly registered with Cisco Smart Software Licensing on Cisco.com.

License Registration Status	Description
Unregistered	Smart Software Licensing is enabled in Cisco EPN Manager but Cisco EPN Manager is not registered with the CSSM.
Registered	Cisco EPN Manager is registered with the CSSM. Cisco EPN Manager has received an ID certificate that will be used for future communication with the Cisco licensing authority.
Registration Expired	Cisco EPN Manager did not successfully renew its registration prior to the expiration date and has been removed from CSSM.

### License Authorization Status

The License Authorization status reflects license usage against purchased licenses, and whether you are in compliance with Cisco Smart Licensing. If you exceed the number of purchased licenses, the product's status will be **Out of Compliance**.

License Authorization Status	Description
Evaluation Mode	Cisco EPN Manager is running in evaluation mode (expires in 90 days).
Authorized	Cisco EPN Manager has a valid Smart Account and is registered. All licenses requested by the product are authorized for use.
Out of Compliance	Cisco EPN Manager has exceeded the number of licenses that were purchased. (Specifically, the virtual account for the product instance has a shortage of one or more licenses types.)
Evaluation Expired	The evaluation period has expired and Cisco EPN Manager is in the unlicensed state.

License Authorization Status	Description
Authorization Expired	Cisco EPN Manager did not successfully renew its license authorization prior to the authorization expiration date.

## Use Traditional Licensing



**Note** Cisco recommends that you convert to Cisco Smart Licensing. See [Set Up Cisco Smart Licensing in Cisco EPN Manager](#), on page 587. If you are using Smart Licensing and want to re-enable traditional licensing, see [Disable Smart Licensing](#), on page 591.

Cisco EPN Manager checks traditional licenses every 4 hours and writes the status to the License log (/opt/CSColumos/logs/license.log). If a time-based license expires, any users that are in an active session will be redirected to the **Licenses** page, and new users are prevented from logging in. If an RTM license device count is exceeded, you should either:

- Delete some of the devices. After the daily inventory collection, the devices will be displayed as **Managed**.
- Obtain a license with a higher RTM count. See [Add and Delete Traditional Licenses](#), on page 593.

See these topics for more information on traditional licenses:

- [Types of Cisco EPN Manager Licenses](#), on page 585
- [View Traditional Licenses](#), on page 593
- [Add and Delete Traditional Licenses](#), on page 593
- [Move a Traditional License to Another Server](#), on page 594

## View Traditional Licenses

To view the traditional Cisco EPN Manager licenses that are currently installed, choose **Administration > Licenses and Software Updates > Licenses**. Cisco EPN Manager supports the licenses listed under **Base License**.



**Note** A separate license is used by each chassis in a multishelf device. For example, if a Cisco NCS 2006 device houses 3 chassis, 3 licenses are used by that device.

## Add and Delete Traditional Licenses

To install a new traditional license, the original license must already reside on the server. Do not create copies of licenses. To purchase new traditional licenses, go to [www.cisco.com/go/license](http://www.cisco.com/go/license). Make sure you install licenses in the correct order. For example, you must always install the Base license first because it is required by the other licenses.

When you delete a license, all of that license's information is removed from the server.

**Caution**

If you make a manual change to a license file, Cisco EPN Manager considers the file corrupted and will not install it. If this happens, obtain a new license file.

**Step 1** Choose **Administration > Licenses and Software Updates > Licenses**.

**Step 2** Choose **Files > License Files**.

- To add a license, click **Add**, click **Choose File**, browse to the location of the license file, and then click **OK**.
- To delete a license, select the license file, then click **Delete**.

## Move a Traditional License to Another Server

The only time you may have to move a license to another server is if you are using high availability, and a server fails. If you need to delete a license, see [Add and Delete Traditional Licenses, on page 593](#). To move the license:

**Step 1** Delete the traditional licenses from the original server.

**Step 2** Send an e-mail to [licensing@cisco.com](mailto:licensing@cisco.com) requesting a *re-host* for your traditional licenses.

**Step 3** When you receive the traditional license, install it on the new server.

## Renewing an Expired License

If your Cisco EPN Manager license has expired, you can complete the following procedure to renew it:

**Step 1** Choose **Administration > Licenses and Software Updates > Licenses**.

The **Licenses** page opens.

**Step 2** Do one of the following:

- If you see the **Summary** and **Files** menus in the top left portion of the page, skip ahead to Step 4.
- If you do not see these menus, you will first need to register traditional licensing. Proceed to Step 3.

**Step 3** Register traditional licensing, then return to Step 1 of this procedure:

- Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.
- With the **Licensing Settings** tab selected, click the **Traditional Licensing** radio button, then click **Register**.
- Log out of Cisco EPN Manager, then log back in.

**Step 4** From the top left area of the page, choose **Files > License Files**.

The **License Files** page opens.

**Step 5** Choose the license file you want to renew:



- a) Click **Add**.

The **Add A License File** dialog box opens.

- b) From the **Select License File** field, click **Choose File**.  
c) Navigate to and click the appropriate license file, then click **Open**.  
d) Click **OK**.

**Step 6** Log out of Cisco EPN Manager, then log back in.

---

## View the Licensing Dashboard

From the **Licensing** dashboard, you can determine whether traditional or smart software licensing is enabled (indicated in the **Active Licensing Mode** field at the top of the dashboard) and view the number of licenses that are currently in use. You can set the licensing mode from the **Smart Software Licensing** page (**Administration > Licenses and Software Updates > Smart Software Licensing**).

To open this dashboard, do one of the following:

- Choose **Administration > Dashboards > Licensing Dashboard**.
- Click the **Licensing Dashboard** link from the top-right corner of the **Smart Software Licensing** page.

The information displayed in the dashboard depends on the licensing mode that is enabled. If smart software licensing is currently enabled, the following dashlets are displayed:

- **License Summary Count** area—Displays the number of licenses consumed and the compliance status for each license type. The number of licenses displayed is based on the current date.
- **License Summary** dashlet—Displays a bar chart that graphs the number of licenses consumed for each license type during a particular time period. To view additional information, place your cursor over the chart.
- **Device Distribution for License** dashlet—To view the device distribution chart for a particular license, click its link from the top of the chart displayed in the **License Summary** dashlet. To view additional information, place your cursor over the chart.



**Note** The information displayed in the **License Dashboard** is refreshed daily after the SmartLicense job runs at 02:00 A.M. (its pre-configured run time). To view this job in the **Job Dashboard**, choose **Administration > Dashboards > Job Dashboard**.

---

If traditional licensing is currently enabled, the **Licensing** dashboard displays the **Traditional Licensing** dashlet. Specify whether you want to view information about Lifecycle or Assurance licenses by choosing the corresponding option from the **License Type** drop-down list. The dashlet updates, displaying information such as the device families with that license type, the number of tokens allocated to each device in those families, as well as the number of tokens that are not being used at the moment.

### Related Topics

[Set Up Cisco Smart Licensing in Cisco EPN Manager](#) , on page 587

[Enable Smart Licensing in Cisco EPN Manager](#) , on page 588

[Register Cisco EPN Manager with the Cisco Smart Software Manager](#), on page 589

[Configure License Thresholds for the Smart License Dashboard](#), on page 591

[Disable Smart Licensing](#), on page 591

[Reference: Smart Product Registration and License Authorization Statuses](#), on page 592

## Manage Software Updates

- [What Are Software Updates?](#), on page 596
- [View the Installed Product Software Version](#), on page 596
- [Enable or Disable Notifications About Software Updates](#), on page 597
- [View Installed Software Updates](#), on page 597

## What Are Software Updates?

Cisco provides updates to the Cisco EPN Manager software periodically. These updates fall into the following three categories:

- **Critical Fixes**—Provide critical fixes to the software. We strongly recommend that you download and apply all of these updates as soon as they are available.
- **Device Support**—Adds support for managing devices which Cisco EPN Manager did not support at release time.
- **Add-ons**—Provide new features, which can include GUI screens and functionality, to supplement the Cisco EPN Manager version you are using. This includes Cisco EPN Manager maintenance packs and maintenance pack point patches.

The update notifications that Cisco EPN Manager displays depend on the Notification Settings specified by your administrator. See [Enable or Disable Notifications About Software Updates](#), on page 597. All software updates are packaged in .ubf files. A large update can contain individual smaller updates, from which you can choose what you want to install. When you install an update, Cisco EPN Manager does the following:

- Verifies that the file publisher is Cisco Systems and the file has not been tampered with
- Automatically installs any other updates that are required

If you have connectivity to <http://www.cisco.com>, you can download and install the updates directly from Cisco.com. If you do not have internet connectivity, copy the update from a server that has the necessary connectivity and install it from there.

See the [Cisco EPN Manager Installation Guide](#) for installation instructions for maintenance packs. For point patch installation instructions, see the readme file provided with the patch file on the Software Download page on Cisco.com.

## View the Installed Product Software Version

Use one of these methods to check the Cisco EPN Manager product version:

- From the Web GUI, click the Settings icon at the top right of the page, and choose **Help > About Cisco EPN Manager**.
- From the CLI, view the contents of the file named  
`#cat /opt/CSColumos/installedComponentsVersions.xml`

To use the CLI, see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).

## View Installed Software Updates

If you are not logged in to the web GUI, you can view a pop-up window that lists the software updates by clicking **View Installed Updates** from the login page.

If you are logged in to the web GUI, you can view the software updates in two ways:

- From the **About Cisco EPN Manager** page, by clicking the settings icon at the top right of the page and clicking **About Cisco EPN Manager**, and then clicking **View Installed Updates**. (The **View Installed Updates** link is also available from the login page.)
- By choosing **Administration > Licenses and Software Updates > Software Update** (this method provides the most detail).

The **Software Update** page displays two tabs:

- **Installed Updates**—Updates that Cisco EPN Manager is currently using.
- **Uploaded Update Files**—Update files that have been uploaded to the server (including those that are not being used). The Corresponding Updates field lists any prerequisite updates that were also uploaded.

If an update file has not yet been installed, it can be deleted. Select the file and click the **Delete** button.

## Enable or Disable Notifications About Software Updates

By default, Cisco EPN Manager displays information about all available updates in the **Software Updates** page. Because the list can be quite long, you may want to adjust what is displayed and the updates for which you are notified. You can also disable all notifications and re-enable them later.

- 
- Step 1** Configure the default Cisco.com credentials so that Cisco EPN Manager can get information about available updates.
- a) Choose **Administration > Settings > System Settings**, then choose **General > Account Settings**.
  - b) Click the **Cisco.com Credentials** tab, enter the credentials, then click **Save**.
- Step 2** Configure your software update notification settings.
- a) Choose **Administration > Settings > System Settings**, then choose **General > Software Update**.
  - b) Under **Notification Settings**, select or deselect the update categories. To disable all notifications, make sure no categories are selected. For an explanation of the categories, see [What Are Software Updates?, on page 596](#)
  - c) Click **Save**.
-





## CHAPTER 21

# Cisco EPN Manager Security

---

This chapter consists of the following topics:

- [Security Overview, on page 599](#)
- [Secure Architecture, on page 599](#)
- [Secure Default Configurations, on page 603](#)
- [Harden Your Installation, on page 603](#)
- [CSDL Process, on page 611](#)

## Security Overview

Cisco EPN Manager requires a high level of security to ensure that your network and its data are not compromised. This is especially important because it has full management control over your network and stores device credentials. To this end, Cisco EPN Manager leverages the following security approaches:

- **Secure architecture:** The Cisco EPN Manager architecture is designed to limit access to any unknown software flaws that may be present so they cannot be used for a malicious purpose.
- **Secure default configurations:** Cisco EPN Manager is shipped with a default configuration that enhances the security of the product. For example, even though insecure FTP and TFTP services are supported, they are not activated in the default configuration.
- **Installation hardening:** Cisco's Advanced Services team can evaluate the specifics of your Cisco EPN Manager installation and complete the additional security hardening tasks that may be needed.
- **Cisco Secure Development Lifecycle (CSDL) process:** From development to release, the CSDL process is followed to improve security of Cisco EPN Manager.

The following sections describe these approaches in more detail.

## Secure Architecture

Cisco EPN Manager's architecture design is based on the premise that 3 conditions must exist simultaneously in order for an attacker to breach a system:

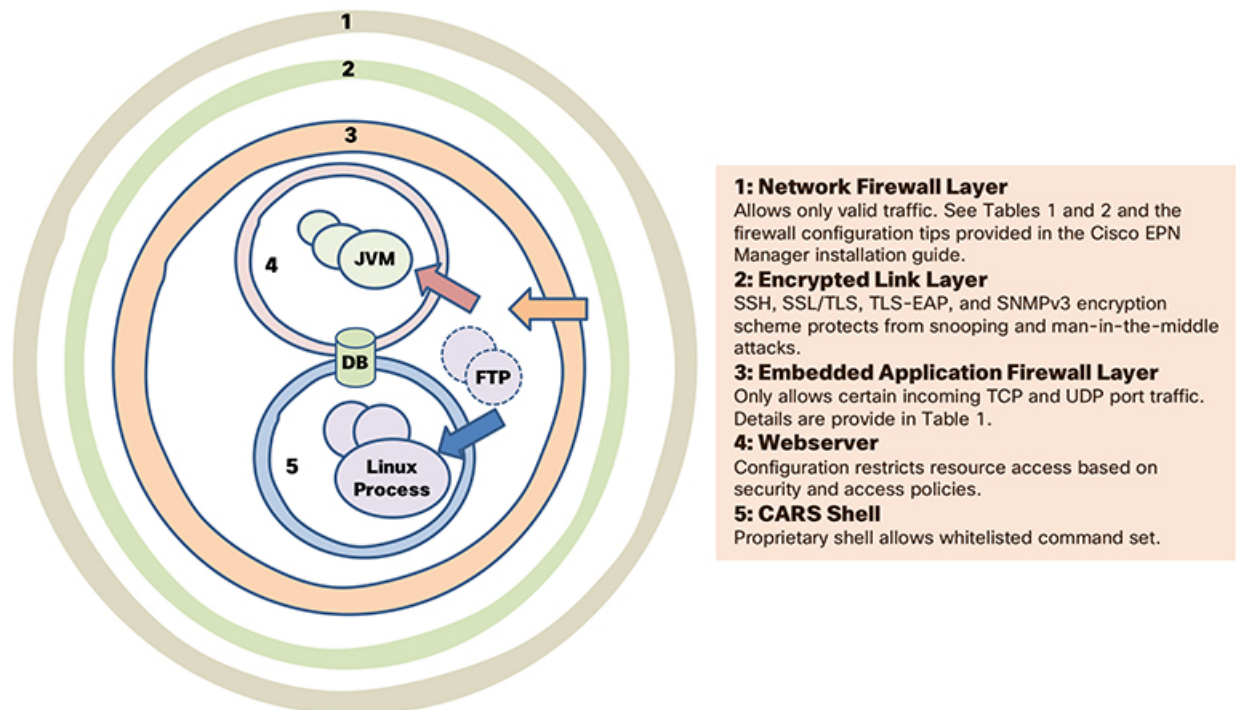
- The system has a flaw.
- The attacker has access to that flaw.

- The attacker is capable of exploiting the flaw for a malicious purpose. (Hughes, J., & Cybenko, G. 2013. Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review*, 3(8): 15-24.)

On its own, a flaw is benign. It is only when an attacker can access the flaw and knows how to exploit it that the flaw becomes a vulnerability. This distinction between a flaw and a vulnerability is important to understand. Just because a flaw has gone public does not automatically mean it has become a vulnerability. And a flaw may only be a vulnerability under certain circumstances.

Limiting access to system flaws is key to the approach Cisco EPN Manager uses to manage security risks. We have designed the Cisco EPN Manager architecture so that any flaws that may be found should not be readily accessible to an attacker. This is a practical and reasonable approach because you cannot always eliminate flaws or prevent an attacker from exploiting them. What you can do is limit access to certain flaws that exist by putting multiple layers of security in place. Cisco EPN Manager uses three layers of perimeter security, as illustrated in Figure 1.

**Figure 3: Multilayer Secured Perimeter Architecture: A Closed System**



Of these three layers, one resides within and two reside outside of Cisco EPN Manager . The interior layer is preconfigured with Cisco EPN Manager and becomes operational after the installation is completed. The two exterior layers are not preconfigured and need to be implemented by creating an exterior network firewall and encrypted communication link layer. We recommend that your company's technical team works with Cisco Advanced Services to create these items.



**Note**

You may need to modify some configurations within Cisco EPN Manager in order to choose the right kind of encryption protocols to use for your network.

The interior layer is built into Cisco EPN Manager and consists of the following components:

- **Embedded firewall**—Provides the first protective layer around the interior components. This allows only a few ports to be open to incoming traffic. This decreases the attack surface by limiting access to multiple flaws (both known and unknown) in the Linux OS and Oracle databases.
- **CARS shell**—Provides a protective layer around Linux by enforcing a whitelist of allowed commands that can be run on Linux, thus restricting interaction with the OS.
- **Web server**—Provides a protective layer around Linux, the Java virtual machine, and the database. This layer has security filters in place for restricting access to Java as well as the database resources and methods.

This interior layer protects the system against many risks, such as the ones described in the following examples. While these flaws are deemed vulnerabilities in an unprotected system, there are not in Cisco EPN Manager. In these examples (identified by their National Vulnerability Database ID), we will assume that the external firewall and encrypted links layer have either been breached by an attacker or are non-existent:

- **CVE-2013-5211: Flaw in NTP's implementation of the Linux NTPD component**—A DoS attack takes place after incoming NTP traffic is accessed from port 23. Since the embedded firewall disallows this traffic, this flaw is not accessible to an attacker and therefore not a risk in Cisco EPN Manager.
- **CVE-2016-0634: Linux bash shell flaw**—This attack can be made by an authenticated user that has targeted a bash shell through port 22. Cisco EPN Manager does not offer direct access to a bash shell via port 22. Instead, a CARS shell is accessible by regular authenticated users. As a result, this flaw is not a risk in Cisco EPN Manager.
- **CVE-2017-12617: Apache Tomcat flaw**—This attack can happen when a PUT request is made. Since Cisco EPN Manager's webserver configuration does not allow this kind of access, this flaw is not a risk.
- **CVE-2015-4863: Oracle database flaw**—This attack can happen on a network via the Oracle Net protocol. This flaw is not a risk in Cisco EPN Manager since the Oracle database resides behind the built-in firewall and webserver. As a result, it is not possible to access the database over the network.

## Ports Used by Cisco EPN Manager

Cisco EPN Manager ships with a built-in application firewall configuration to ensure that only legitimate traffic is allowed into the server. Table 1 lists the ports used to listen for connection requests from devices and accept incoming traffic. The opening and closing of these ports in the firewall is done automatically by Cisco EPN Manager when you enable or disable certain features. There is no need to enable or disable the ports within the firewall. If you try to specify any firewall configurations that circumvent Cisco EPN Manager, you may compromise its security and integrity.



### Note

Table 1 also provides information required to carry out post-installation security hardening (see [Secure Default Configurations](#) for more information).

Table 44: Listening Ports That Are Open Through Built-in Firewall

Port	Protocol	Usage	Safe to Disable?	Notes
21	TCP	To transfer files to and from devices using FTP.	Yes	Disable FTP from the web GUI under <b>Administration &gt; Settings &gt; System Settings</b> , then choose <b>General &gt; Server</b> . After disabling FTP, as the CLI admin user, stop and restart the server.
22	TCP	To initiate SSH connections with the Cisco EPN Manager server, and to copy files to the Cisco EPN Manager server using SCP or SFTP.	Depends	This might be still needed by older managed devices that only support TFTP and not SFTP or SCP.
69	UDP	To distribute images to devices using TFTP.	Depends	Only if alternative protocols like SCP or SFTP or HTTPS are used for image distribution, and if supported by the managed devices.
162	UDP	To receive SNMP traps from network devices.	No	—
443	TCP	For browser access to the Cisco EPN Manager server via HTTPS.	No	—
514	UDP	To receive syslog messages from network devices.	No	—
1522	TCP	For High Availability (HA) communication between active and standby Cisco EPN Manager servers. Used to allow Oracle JDBC traffic for Oracle database synchronization.	Yes	If at least one Cisco EPN Manager server is not configured for HA, this port is automatically disabled.
2021	TCP	To distribute images to devices using FTP.	No	—
8082	TCP	For the HA Health Monitor web interface (via HTTP). Used by primary and secondary servers to monitor their health status via HTTP.	No (If HA configured)	—
8087	TCP	To update software on the HA secondary backup server (uses HTTPS as transport).	No	—



Port	Protocol	Usage	Safe to Disable?	Notes
9991	UDP	To receive Netflow data packets.	Yes	Cisco EPN Manager does not support Netflow. You should disable this traffic in the network firewall.
9992	TCP	To manage M-Lync using HTTP or HTTPS.	Yes	Cisco EPN Manager does not support M-Lync. You should disable this traffic in the network firewall.
11011 to 11014	TCP	For PnP operations for proprietary Cisco Network Service (CNS) protocol traffic.	Yes	Cisco EPN Manager does not support PnP. You should disable this traffic in the network firewall.
61617	TCP	For MTOSI NBI notification over Java Message Service (JMS) connections. Also used for PnP operations.	Yes	Cisco EPN Manager does not support MTOSI over JMS or PnP. You should disable this traffic in the network firewall.

## Secure Default Configurations

Cisco EPN Manager ships with default application configurations that are as secure as possible. You should only modify them after you have analyzed the threat model and assessed the risks for your specific situation. With the default configurations, Cisco EPN Manager does its best to:

- Not use default passwords.
- Not make unnecessary OS and Oracle packages/services accessible.
- At the time of a Cisco EPN Manager release, the latest security patches are applied for the embedded OS and Oracle.
- Not allow the use of Oracle access passwords by human users. These passwords are machine-generated and used by internal components.

## Harden Your Installation

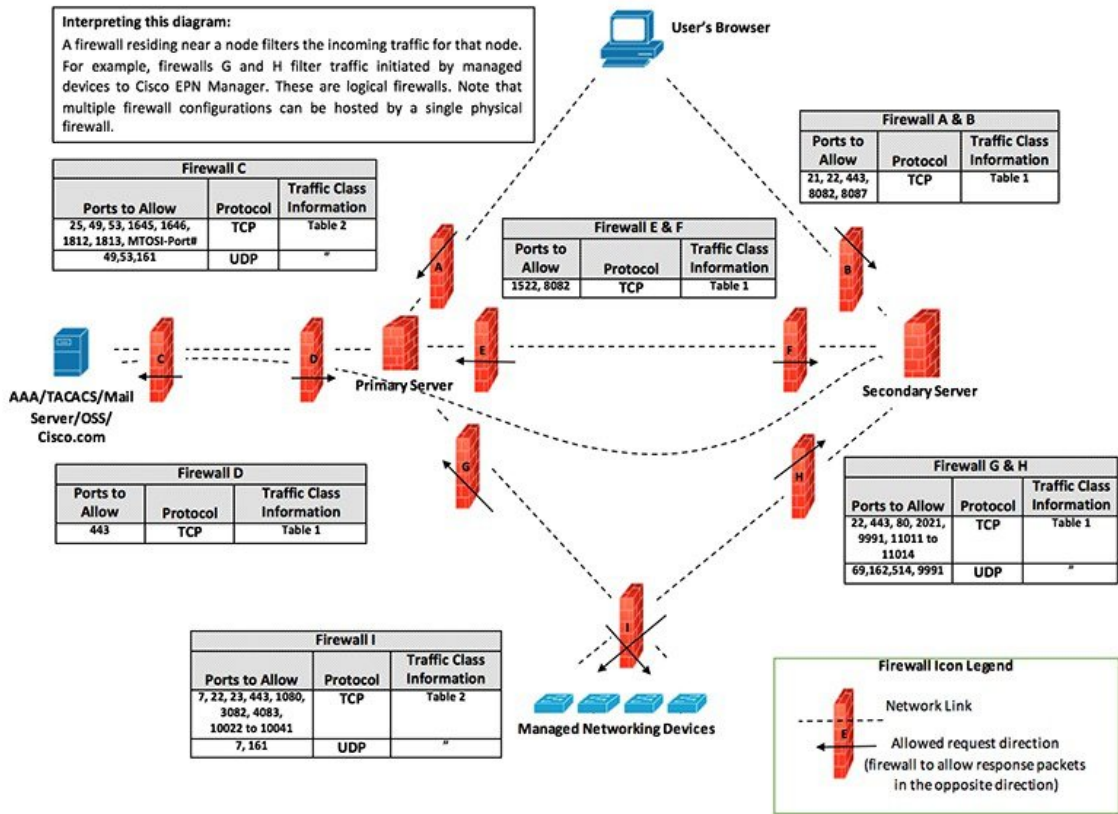
To harden your Cisco EPN Manager installation, you need to complete the following tasks:

1. Configure the built-in interior and exterior network firewalls to allow only legitimate traffic.
2. Use encryption for all incoming and outgoing traffic.
3. Configure Cisco EPN Manager and its peer systems to allow the transmission of only legitimate transactions.

Before you proceed, you should first understand how Cisco EPN Manager interacts with peer systems. This, along with management traffic flows and the exterior network firewalls for a generic HA deployment, is illustrated in the following figure.



**Note** Although we recommend that you implement these firewalls, you are not required to do so.



Depending on your installation, you may need to customize the firewall configuration to further improve security. As a general policy, any ports that are not needed and not secure (i.e. do not transmit encrypted traffic) should be disabled.

# Configure the Built-In Application Firewall

To configure the application firewall, you need to disable the Cisco EPN Manager features that your installation does not need to run. This will automatically shut down the corresponding listening ports in the firewall.

- Step 1** Identify the ports that are currently enabled:
- To view a list of the ports used in your deployment that are exposed externally, log in as a Cisco EPN Manager CLI admin user and then run the **show security-status** command.
  - To view a list of all open listening ports at the OS level, including those that are blocked by the built-in firewall, log in as the Linux CLI admin user and then run the **netstat -aln** command.

**Step 2** Using Table 1 for guidance, determine which of these ports can be safely disabled without disrupting the normal functioning of Cisco EPN Manager .

Note the following:

- Cisco EPN Manager uses some of the listening ports for its internal operations. These ports are kept hidden behind the built-in firewall.
- You should only use the procedure provided in Table 1 to enable or disable ports.

## Set Up Exterior Network Firewalls

In addition to the built-in firewall, you can also deploy network firewalls that only allow traffic targeted at the listening ports used by Cisco EPN Manager and its peer systems. The figure provided in the [Harden Your Installation](#) topic illustrates how the port information listed in Tables 1 and 2 are used to set up firewall rules. Use this figure to decide on the appropriate firewall configurations for your management network.

- To identify the traffic class, refer to the **Usage** column in Table 1. We recommend that you disable the ports used by the services that are not used by your Cisco EPN Manager installation.
- You should also enable the destination ports that Cisco EPN Manager uses for outgoing traffic (to connect to network devices or peer systems) in your network firewalls. Refer to Table 2 for a listing of these destination ports and their purpose.

**Table 45: Destination Ports Used by Cisco EPN Manager**

Port	Protocol	Used to:
7	TCP/UDP	Discover endpoints using ICMP.
22	TCP	Initiate SSH connections with managed devices.
23	TCP	Communicate with managed devices using Telnet.
25	TCP	Send email using an SMTP server.
49	TCP/UDP	Authenticate Cisco EPN Manager users using TACACS.
53	TCP/UDP	Connect to DNS service.
161	UDP	Poll using SNMP.
443	TCP	Upload or download images and perform configuration backup-restore for Cisco NCS 2000 devices using HTTPS.
1522	TCP	Communicate between primary and secondary HA servers (allows Oracle JDBC traffic for Oracle database synchronization between primary and secondary servers).
1080	TCP	Communicate with Cisco Optical Networking System (ONS) and Cisco NCS 2000 series devices using Socket Secure (SOCKS) protocol.

Port	Protocol	Used to:
1645, 1646, and 1812, 1813	UDP	Authenticate Cisco EPN Manager users using RADIUS.
3082	TCP	Communicate with Cisco ONS and Cisco NCS 2000 devices using TL1 protocol.
4083	TCP	Communicate with Cisco ONS and Cisco NCS 2000 series devices using TL1 protocol.
8082	TCP	Communicate between primary and secondary HA servers to monitor each other's health using HTTPS.
10022 to 10041	TCP	Passive FTP file transfers (for example, device configurations and report retrievals).
<i>MTOSI/RESTCONF TCP port number</i>	TCP	Listen at NBI client connected to the Cisco EPN Manager server (after this port is configured by NBI client system, a registration notification message containing the port number is sent to Cisco EPN Manager server); refer to the <a href="#">MTOSI or RESTCONF API guide</a> for more information.

## Set Up Traffic Encryption

You will need to encrypt the following traffic groups:

- Northbound traffic—This group consists of either client-server traffic from a human user's browser or NBI traffic from a Business Support System/Operational Support System (BSS/OSS). This traffic is transmitted over HTTP, so you need to implement HTTPS (HTTP encrypted by TLS). For a description of how to set up HTTPS, see [Set Up HTTPS to Secure the Connectivity of the Web Server](#).
- Southbound traffic—This group consists of management traffic that queries or configures managed devices using a wide range of protocols such as SNMP and HTTP. Protocols such as SSH and SNMPv3 may be used to secure this traffic. For a description of the configuration steps that need to be completed in order to encrypt this traffic, see [Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices](#).
- East-West traffic between peer systems—This group consists of traffic between Cisco EPN Manager and a variety of other supporting systems like an external authentication server (secured by TLS-EAP) or a SMTP mail server (secured by TLS). Different encryption protocols are used, depending on the application protocol that needs to be protected. Some of the application protocols may also have built-in encryption.
- East-West traffic between a primary and secondary server in an HA deployment—This group consists of traffic between two Cisco EPN Manager servers running in primary and secondary mode. Each server monitors the other's health and keeps database and other file content synchronized over a connection secured by HTTPS.

## Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices

SNMPv3 is a higher security protocol than SNMPv2. If your devices support SNMPv3, configure the devices to use SNMPv3 to communicate with the Cisco EPN Manager server. The following procedures explain how to specify SNMPv3 when adding new devices.

Method for Adding Devices	How to Specify SNMPv3	For more information, see:
Add a single device	In the <b>Add Device</b> dialog box, go to the <b>SNMP Properties</b> page and choose <b>v3</b> from the <b>Versions</b> drop-down list.	<a href="#">Add Devices Manually (New Device Type or Series), on page 50</a>
Add multiple devices (bulk import)	When you edit your CSV file, enter the following: <ul style="list-style-type: none"> <li>• Enter <b>3</b> in the <b>SNMP Version</b> column.</li> <li>• Enter the appropriate values for these columns: <b>snmpv3_user_name</b>, <b>snmpv3_auth_type</b>, <b>snmpv3_auth_password</b>, <b>snmpv3_privacy_type</b>, and <b>snmpv3_privacy_password</b></li> </ul>	<a href="#">Import Devices Using a CSV File, on page 49</a>
Add multiple devices using discovery	In the <b>Discovery Settings</b> dialog box, go to the <b>Credential Settings</b> area and click <b>SNMPv3 Credentials</b> . Click the + sign to add the device credentials.	<a href="#">Run Discovery With Customized Discovery Settings, on page 47</a>

### Before you begin

Make sure SNMPv3 is enabled (with the appropriate security algorithm, such as HMAC-SHA-96) on the network devices that support it.

## Set Up External Authentication Using the CLI

We recommend that you manage user accounts and passwords using a dedicated, remote authentication server running a secure authentication protocol such as RADIUS or TACACS+. In addition to setting up authentication using the following procedure, contact your external authentication vendor for additional security hardening suggestions.



### Note

If you decide to use local user authentication, check the default password policies to determine whether you want to make them stronger. See [Configure Global Password Policies for Local Authentication, on page 681](#).

Configure Cisco EPN Manager to authenticate users using an external AAA server. You can configure the server using the web GUI or by using the command line interface (CLI). To set up remote user authentication via the GUI, see [Configure External Authentication, on page 691](#).

To configure external authentication using the CLI, follow these steps. In this example, external authentication will be done by an external TACACS+ server.

**Step 1** Log in to Cisco EPN Manager using the command line, as explained in [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).

**Step 2** Enter config mode.

**Step 3** Enter the following command to setup an external authethn TACACS+ server:

```
aaa authentication tacacs+ server tacacsIP key plain shared-secret
```

Where:

- *tacacsIP* is the IP address of an active TACACS+ server.
- *shared-secret* is the plain-text shared secret for the active TACACS+ server.

**Step 4** Enter the following command to create a user with administrator privileges, who will be authenticated by the server specified in the previous step:

```
username username password remote role admin [email emailID]
```

Where:

- *username* is the name of the user ID.
- *password* is the plain-text password for the user.
- *emailID* is the email address of the user (optional).

## Harden SSH Against Brute-Force Password Attacks

Since password-based SSH authentication is vulnerable to brute-force attacks, we recommend that you switch to RSA key-based SSH authentication after installing Cisco EPN Manager . To make the switch, do the following:

**Step 1** Log in as the Linux CLI admin user:

- Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
- Run the following command: **shell**
- Enter the shell access password.

**Step 2** Check who the current user is:

```
# whoami
```

The resulting output should indicate that you are the Linux admin user, not the Linux root user.

**Step 3** For the Cisco EPN Manager admin user, create RSA key pairs and an SSH string using a tool (such as puTTYgen) with at least 2048-bit strength.

The SSH string should look something like this:

```
ssh-rsa AAAAB3NzaC1y ... 0Q== rsa-key-20180128
```

**Tip** Save the private key in a file, preferably in encrypted form with a passphrase. Also keep the passphrase handy.

- Step 4** Create the `authorized_keys` file and assign the appropriate access privileges to the Cisco EPN Manager admin user:
- In the admin user's home directory, create the `.ssh` directory and assign read, write, and execute privileges for this directory to only the admin user:

```
# cd ~
# mkdir .ssh
# chmod 700 ~/.ssh
```

- Create the authorized keys file:

```
# cd .ssh
# vi authorized_keys
```

- Copy and paste the SSH string you created in Step 3 in to the `authorized_keys` file and then save the file.
- Assign read, write, and execute privileges for the `authorized_keys` file to only the admin user:

```
# chmod go= ~/.ssh/authorized_keys
# chmod u=rwx ~/.ssh/authorized_keys
```

- Confirm you assigned the appropriate access privileges to the `authorized_keys` file:

```
# ls -al
```

The resulting output should look something like this:

```
total 6
drwx-----. 2 admin gadmin 1024 May 10 00:25 .
drwx-----. 6 admin gadmin 1024 May 10 00:24 ..
-rwx-----. 1 admin gadmin 398 May 10 00:25 authorized_keys
```

In this example, the Linux admin user is named `admin`

- Step 5** Switch to the root user in a bash shell:

```
# sudo -i
```

- Step 6** Update the `sshd_config` file:

- Copy the current and original versions of the `sshd_config` file, located in the `/etc/ssh` directory:

```
# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig
```

- Open the `sshd_config` file in a vi editor:

```
# vi /etc/ssh/sshd_config
```

- Enter the following key-value pairs by creating new entries or changing existing entries as needed:

```
Protocol 2
KeyRegenerationInterval 1h
ServerKeyBits 2048
MaxAuthTries 4
PasswordAuthentication no
PermitRootLogin no
AuthenticationMethods publickey
PubkeyAuthentication yes
```

- Save the file.

- Step 7** Reload `sshd`:

```
# systemctl reload sshd.service
```

**Caution** Do not restart `sshd`. If any of the previous configuration steps are not completed correctly and you restart `sshd`, you will lose access to SSH. It is much safer to reload `sshd` because current SSH sessions are maintained (allowing you to make any necessary corrections).

The configuration of RSA key-based SSH authentication is complete. To confirm that configuration was successful, keep the existing SSH session open (in case you need to fix something) and try to open a new SSH session using the private key and passphrase you created in Step 3 of this procedure.

## Harden NTP

Network Time Protocol (NTP) authenticates server date and time updates. We recommend you configure the Cisco EPN Manager server to perform time synchronization over NTP. Failure to manage NTP synchronization across your network can result in anomalous results. Management of network time accuracy is an extensive subject that involves your organization's network architecture and falls outside the scope of this guide. For more information on this topic, see (for example) the Cisco white paper [Network Time Protocol: Best Practices](#).

Note the following:

- Because using NTP creates the possibility of security breach-related disruptions, you should also harden the NTP aspect of the Cisco EPN Manager server by using NTP version 4 (NTPv4). Cisco EPN Manager also supports NTPv3 because NTPv4 is backward compatible with NTPv3.
- You can configure a maximum of 3 NTP servers with Cisco EPN Manager .

## Set Up NTP on the Cisco EPN Manager Server

To use the Network Time Protocol (NTP) to synchronize clocks on the server and network devices using an NTP server, NTP must first be set up on the Cisco EPN Manager server. For information on how to do this, see [Set Up NTP on the Server, on page 644](#).

## Enable Authenticated NTP Updates

Complete the following procedure to set up authenticated NTP updates:

**Step 1** Log in to Cisco EPN Manager using the command line, as explained in [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).

**Step 2** Enter config mode.

**Step 3** Enter the following command to setup an external NTPv4 server:

```
ntp server serverIP userID plain password
```

Where:

- *serverIP* is the IP address of the authenticating NTPv4 server you want to use.
- *userID* is the md5 key id of the NTPv4 server.
- *password* is the corresponding plain-text md5 password for the NTPv4 server.

For example:

```
ntp server 209.165.202.128 20 plain myPass123
```



**Step 4** Perform these tests to ensure NTP authentication is working correctly:

a) Check the NTP update details:

```
show run
```

b) Check NTP sync details:

```
show ntp
```

---

## Configure External NFS-Based Storage Servers

NFS servers may be used as external storage in a Cisco EPN Manager installation, especially for data backup. Since NFS does not have built-in security, you must implement as many of the following security measures as possible to secure the NFS server:

- Set up a firewall in front of the NFS server—To do this practically, tie down the ports that NFS will use in various configuration files and then specify those ports in the firewall configurations.
- Use a port mapper—On the NFS server, only allow NFS transactions that involve specific IP addresses.
- To prevent attacks via a compromised DNS, only specify IP addresses (and not domain names) when configuring NFS.
- When setting up the export of folders, use the **root\_squash** option in the `/etc/exports` file.
- When configuring the `/etc/exports` file, use the **secure** option.
- When configuring the backup staging and storage folders, use the **nosuid** and **noexec mount** options.



---

**Note** It is not mandatory to configure a staging folder.

---

- For the storage folder (and optional staging folder), configure a file access permission value of **755** (which grants all users read and write privileges) and set userid **65534** (the user **nobody**, who does not have any system privileges) as the owner.
- Tunnel NFS traffic either through SSH or SSL/TLS. For SSH, use RSA key-based authentication instead of user authentication.

Do not rely on just one of these measures to secure your NFS-based storage. Your best bet is to implement the combination of measures that best suits your situation. Also keep in mind that this list is not an exhaustive one. To achieve a higher level of confidence when hardening your storage, we recommend that you discuss your situation with a Linux system admin and a security expert beforehand.

## CSDL Process

Cisco EPN Manager development adheres to the Cisco Secure Development Lifecycle (CSDL) process. This covers the entire development-to-deployment timespan to improve product and installation security. Cisco EPN Manager's product design is reviewed from a security viewpoint against specific criteria and the product

is tested using security tools and test methods. In addition, Cisco EPN Manager is reviewed by external security experts and penetration testers. See [Cisco Security Issue Resolution Process](#) for a description of how security fixes are deployed (as part of the Cisco EPN Manager update lifecycle).

## Cisco Security Issue Resolution Process

There are 2 types of defects and vulnerabilities: customer-found and Cisco-found. Let's cover how Cisco addresses them for Cisco EPN Manager .

### Customer-Found Defects and Vulnerabilities

1. After a customer raises a service request with the Cisco Technical Assistance Center (TAC), the Cisco TAC opens a case with the support team who (depending on the problem) may open a Cisco Defect and Enhancement Tracking System (CDETS) defect report.
2. Cisco evaluates the defect to determine whether that defect poses a security risk to Cisco EPN Manager . If the defect does pose a security risk, then Cisco categorizes it as a vulnerability. Otherwise, Cisco treats the defect as a regular software defect.
3. Cisco does one of the following:
  - For security vulnerabilities, Cisco reports it to the Cisco Product Security Incident Response Team (PSIRT), develops a fix that adheres to Cisco PSIRT guidelines, and then allows Cisco PSIRT to handle both the disclosure of the vulnerability to the client and delivery of the patch.
  - For defects, Cisco determines its severity and schedules the release of a fix.

### Cisco-Found Defects and Vulnerabilities

For the first year following the end-of-sale date for a Cisco EPN Manager version, Cisco provides bug fixes, maintenance releases, workarounds, or patches for critical bugs and security vulnerabilities reported via the TACS or Cisco.com Web site.



## CHAPTER 22

# Backup and Restore

---

- [Backup and Restore Concepts, on page 613](#)
- [Set Up and Manage Repositories, on page 618](#)
- [Set Up Automatic Application Backups, on page 623](#)
- [Perform a Manual Backup, on page 625](#)
- [Restore Cisco EPN Manager Data, on page 626](#)
- [Manage Disk Space Issues During Backup and Restore, on page 629](#)
- [Migrate to Another Virtual Appliance Using Backup and Restore, on page 629](#)

## Backup and Restore Concepts

- [Backup Types: Application and Appliance, on page 613](#)
- [Backup Scheduling, on page 614](#)
- [Backup Repositories, on page 614](#)
- [Backup Filenames, on page 615](#)
- [Backup Validation Process, on page 615](#)
- [Information That Is Backed Up, on page 616](#)
- [Information That Is Not Backed Up, on page 618](#)

## Backup Types: Application and Appliance

Cisco EPN Manager supports two types of backups:

- **Application backups**—These contain Cisco EPN Manager application data but do not include host-specific settings, such as the server hostname and IP address.
- **Appliance backups**—These contain all application data and host-specific settings, including the hostname, IP address, subnet mask, and default gateway.

Note the following about application and appliance backups.

- Application and appliance backups can be restored to the same or a new host, as long as the new host has the same hardware and software configuration as the host from which the backup was taken.
- You can only restore an appliance backup to a host running the same version of the Cisco EPN Manager server software as the server from which the backup was taken.

- When upgrading to a later version of Cisco EPN Manager , application backup and restore can run across different releases, as long as the upgrade path is supported.
- You cannot restore an application backup using the appliance restore command, nor can you restore an appliance backup using the application restore command.

We recommend the following best practices:

- If you are *evaluating* Cisco EPN Manager , use the default automatic application backup to the local repository.
- If you are running Cisco EPN Manager *in a production environment* as a virtual appliance, take regular application backups to a remote backup server. You can use the application backups to restore your server for all failures except complete failure of the server hardware.

## Backup Scheduling

Cisco EPN Manager performs automatic scheduled application backups. This feature is enabled by default and creates one application backup file every day in the default local backup repository.

You can change this schedule as needed. You can also take an automatic application backup at any time from the web GUI. Appliance backups can only be taken from the command line.

Automatic application backups can create storage space problems if the backup repository is local to the Cisco EPN Manager server. While this is usually acceptable in test implementations, it is not intended to substitute for routine scheduled backups to remote servers in a production environment.

We recommend the following for production environments:

- Set up remote repositories to store the backup files.
- Use the automatic schedule application backup to create backups on the remote repositories on a regular schedule.

Even if you are using scheduled backups, you can still use the command line to create application or appliance backups at any time.

## Backup Repositories

By default, automatic application backup feature stores backup files in the local backup repository **/localdisk/defaultRepo**. You can use the web GUI to create a new local backup repository and then choose it when you set up automatic application backups. You can also specify a remote repository but you must create the repository first as described in [Set Up and Manage Repositories, on page 618](#).

When taking application or appliance backups using the command line, you must specify the local or remote repository you want the backup to be stored in. In a production environment, this is normally a remote repository that is accessed via NFS, SFTP, or FTP. We recommend you use NFS because it is typically much faster and more reliable than other protocols.

There is no difference between performing an application backup from the command line or performing it from the web GUI. Both actions create the same backup file.

Whenever you use NFS to take backups or restore data from a remote backup, make sure the mounted NFS server remains active throughout the backup or restore operation. If the NFS server shuts down at any point in the process, the backup or restore operation will hang without warning or an error message.

## Backup Filenames

**Application backups launched from the web GUI**—either automatically or manually—are assigned a filename with the following format:

*host-yymmdd-hhmm\_VERver\_BKSZsize\_CPUcpus\_MEMtarget\_RAMram\_SWAPswap\_APP\_CKchecksum.tar.gpg*

**Application backups launched from the CLI** use the same format, except that the file starts with the user-specified filename rather than the server name.

*filename-yymmdd-hhmm\_VERver\_BKSZsize\_CPUcpus\_MEMtarget\_RAMram\_SWAPswap\_APP\_CKchecksum.tar.gpg*

**Appliance backups launched from the CLI** have files that also start with the user-specified filename, but the type is indicated as SYS, not APP.

*filename-yymmdd-hhmm\_VERver\_BKSZsize\_CPUcpus\_MEMtarget\_RAMram\_SWAPswap\_SYS\_CKchecksum.tar.gpg*

The following table describes the variables used by the backup files.

Variable	Description
<i>host</i>	Host name of the server from which the backup was taken (for application backups launched from web GUI).
<i>filename</i>	Filename specified by user in command line (for application backups launched from CLI, and for appliance backups)
<i>yymmdd-hhmm</i>	Date and time the backup was taken
<i>ver</i>	Internal version.
<i>size</i>	Total size of the backup
<i>cpus</i>	Total number of CPUs in the server from which the backup was taken
<i>target</i>	Total amount of system memory in the server from which the backup was taken
<i>ram</i>	Total amount of RAM in the server from which the backup was taken
<i>swap</i>	Total size of the swap disk on the server from which the backup was taken
<i>checksum</i>	Backup file checksum

## Backup Validation Process

Cisco EPN Manager performs the following steps to validate the backup files:

1. Before starting the backup process, validates disk size, fast-recovery area, and control files.
2. Validates the created backup database to ensure that it can be restored.
3. Validates the zipped application data against the files that were backed up.
4. Validates the TAR file to make sure it is correct and complete.
5. Validates the GPG file to ensure that it is correct.

If you manually transfer the backup file, or if you want to verify that the backup file transfer is completed, view the file's md5Checksum and file size.

Another best practice for validating a backup is to restore it to a standalone "test" installation of Cisco EPN Manager .

## Information That Is Backed Up

The following table describes the information that is contained in backup files. This information is restored to the server from backups.

See [Information That Is Not Backed Up, on page 618](#) for details about data that is not saved by the backup mechanism.

**Note**

The /opt/CSColumos/conf/Migration.xml file contains all configuration files and reports that are backed up. This file is included in the backup and is restored.

Data Type	Feature	Information Saved and Restored
-----------	---------	--------------------------------

Application Data	Background job settings	Data in the database
	Configuration archive (device configuration files)	Data in the database
	Configuration templates	<ul style="list-style-type: none"> <li>Files in /opt/CSCOlumos: <ul style="list-style-type: none"> <li>/conf/ootb</li> <li>/xmp_inventory/dar/customized-feature-parts/CONFIGURATION</li> </ul> </li> <li>Data in the database</li> </ul>
	Credentials	Data in the database
	Device inventory data	Data in the database
	Licenses	Files in /opt/CSCOlumos/licenses
	Maps	<ul style="list-style-type: none"> <li>Files in /opt/CSCOlumos/domainmaps</li> <li>Data in the database</li> </ul>
	Reports	<ul style="list-style-type: none"> <li>Files in /localdisk/ftp: <ul style="list-style-type: none"> <li>/reports</li> <li>/reportsOnDemand</li> </ul> </li> <li>Data in the database</li> </ul>
	Managed device software image files	Data in the database
	System settings	Data in the database
	User preferences	<ul style="list-style-type: none"> <li>Files in /opt/CSCOlumos/conf/wap/datastore/webacs/xml/prefs</li> <li>Data in the database</li> </ul>
	CEPNMusers, groups, and roles	Data in the database
	Virtual domains	Data in the database

Platform Data	CLI settings	All CLI information and settings are preserved. This includes the list of backup repositories, the FTP user name, users created using the CLI, AAA information specified via the CLI, and other CLI settings (such as the terminal timeout).
	Credentials	Linux OS credentials file
	Network settings	Files in /opt/CSColumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml
	Linux user preferences	Linux data structure
	Linux users, groups, and roles	Linux data structure

## Information That Is Not Backed Up

Before performing a backup, make sure that you manually note the following information because it is not saved as part of the backup process. You will need to reconfigure these settings after the data has been restored.

- High availability configurations
- Local customization (for example, report heap size)

Patch history information is also not saved.

For a list of information that is backed up, see [Information That Is Backed Up, on page 616](#).

## Set Up and Manage Repositories

Cisco EPN Manager supports the following repository types:

- Local repositories—NFS
- Remote repositories—NFS, FTP, SFTP

See the following topics for information on how to set up and manage these different types of repositories.

## Create a Local Backup Repository

Cisco EPN Manager stores automatic backup files in the default local backup repository `/localdisk/defaultRepo`. You can create a different local backup repository and use it if you prefer.

- 
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
  - Step 2** Choose **System Jobs > Infrastructure**.
  - Step 3** In the Jobs list, check the **Server Backup** check box.
  - Step 4** Click **Edit** (the pencil icon) to open the Edit Job Properties dialog box.
  - Step 5** Create the new local repository using the Edit Job properties dialog box.



1. Click **Create**. The Create Backup Repository dialog box opens.
2. Enter the name of the local repository you want to create.
3. If it is an FTP repository, check the **FTP** check box and enter the location and credentials.
4. Click **Submit**. The new repository is added to the Backup Repository drop-down list in the Edit Job Properties dialog box.

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

**Step 7** If you want to use the repository for future automatic application backups, specify it as described in [Specify the Backup Repository for Automatic Backups, on page 624](#).

---

## Use a Remote Backup Repository

In production environments, we recommend that you use remote repositories for backups so that your network management data is protected from hardware and site failures. In most cases, this means you will need to:

1. Create one or more remote repositories to hold Cisco EPN Manager backup files. You will need to set these up yourself if your organization does not already have remote backup servers.
2. Specify the remote repository as the destination for automatic application backups.
3. If needed, specify the interval between automatic application backups and time of day to take them. You will need to monitor and manually archive automatic application backups stored on remote repositories (because the **Max backups to keep** setting does not apply to remote repositories).
4. Specify the remote repository as the backup destination when taking an application or appliance backup using the CLI backup commands.

As with any resource that you plan to access remotely, specifying the correct server IP address and login credentials during setup are a requirement for successful use of remote backup repositories with Cisco EPN Manager .

## Use Remote NFS Backup Repositories

To use NFS-based remote backup repositories, you need an NFS file server (which exports the designated folders in its file system to its client) and Cisco EPN Manager (which acts as the server's client). The Cisco EPN Manager system mounts the exported folders and makes them, along with other local folders, available to the Cisco EPN Manager server. To set this up, complete the following three tasks:

1. Specify the paths for the two folders on the NFS server that will stage and store backups, then configure the NFS server to export these paths. Since this falls outside of the scope of Cisco EPN Manager setup, this task should be completed by the NFS server's system admin.
2. Set up Cisco EPN Manager to use the staging and storing folders you specified. This should be completed by a Cisco EPN Manager admin.
3. Secure communication between the NFS server and Cisco EPN Manager, which is very important because NFS is not secure on its own. This should be completed by a Linux admin who has a solid understanding of the security issues that NFS and its installation entails. For tips on hardening NFS, see [Harden NFS-Based Storage](#).

## Before You Set Up the NFS Backup Configuration

Before you begin, make sure:

- You know the IP address of the NFS server on which you want to stage and store backups. The staging and storage folders can be on the same NFS server, or on separate NFS servers. If you plan to stage and store on separate NFS servers, you will need IP addresses for both servers.
- You know the path names of the staging and storage folders on the NFS server. If you choose to stage and store on the same NFS server, the staging and storage folders *must* have different names.
- You have an administrator user ID with root privileges on the Cisco EPN Manager server.
- You have selected a repository name on the Cisco EPN Manager server, which will point to the NFS server storage folder.

## Set Up NFS-Based Remote Repositories

Complete the following procedure to set up the NFS-based remote repositories that Cisco EPN Manager will use for backups.

- 
- Step 1** Log into the server as the Cisco EPN Manager CLI admin user. See [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).
- Step 2** Enter configuration mode:
- ```
configure terminal
config#
```
- Step 3** Set up the NFS remote repositories that will stage the temporary files created during backup processing and store completed backup files:
- ```
config# backup-staging-url nfs://Staging_Server_IP_Address:/Staging_Server_Path
config# repository repositoryName
config-Repository# url nfs://Storage_Server_IP_Address:/Storage_Server_Path
```

Where:

- *Staging\_Server\_IP\_Address* is the IP address of the NFS server on which the staging repository is located.
- *Staging\_Server\_Path* is the full path of the staging repository on its host NFS server.
- *repositoryName* is the name of the remote repository that will store completed backup files.
- *Storage\_Server\_IP\_Address* is the IP address of the NFS server on which the storage repository is located.
- *Storage\_Server\_Path* is the full path of the storage repository on its host NFS server.

**Caution** We recommend that you only enter an IP address for *Staging\_Server\_IP\_Address* and *Storage\_Server\_IP\_Address*. If the DNS service has been compromised and you enter a URL instead, this can result in the redirection of traffic to a malicious NFS server. That said, if you still prefer to specify a URL, we suggest you configure Cisco EPN Manager to use local name resolution (instead of relying on the DNS service). This can be done by entering the NFS server's name and IP address in the */etc/hosts* file. Doing so can improve system security.

- Step 4** Exit configuration mode:

```
config-Repository# exit
config# exit
```

## Use Remote FTP Backup Repositories



**Note** We recommend using remote NFS repositories.

You can create backup repositories on a remote FTP server and configure the Cisco EPN Manager server to use them.

The FTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Cisco EPN Manager server.
- Has a user (FTP user) with write access to the FTP server disk.
- Has a local subdirectory that matches the repository name you specify on the Cisco EPN Manager server.
- Has a password of 16 characters or less.

Other than these requirements, no other configuration is needed on the FTP backup server.

For the SFTP server details to appear in the **Backup Repository** drop-down list in the web GUI, you should configure the FTP server using the CLI. You can configure the FTP server only using the CLI.

**Step 1** Log into the server as the Cisco EPN Manager CLI admin user. See [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).

**Step 2** Enter configuration mode:

```
configure terminal
config#
```

**Step 3** Configure a symbolic link to the remote FTP server, then exit configuration mode:

```
config# repository repositoryName
config-Repository# url ftp://RemoteServerIP//sharedFolder
config-Repository# user userName password plain userPassword
config-Repository# exit
config# exit
```

Where:

- *repositoryName* is the name of the repository (for example, **MyRepo** or **EPNManager**).
- *RemoteServerIP* is the IP address of the FTP server hosting the shared backup folder.
- *sharedFolder* is the name of the shared backup folder on the FTP server.
- *userName* is the name of the user with write privileges to the repository on the FTP server.
- *userPassword* is the corresponding password for that user. The password must be 16 characters or less.

**Step 4** Verify the creation of the symbolic link:

```
show repository repositoryName
```

### What to do next

When you perform a manual backup, specify the new repository as the repository name in the backup command. For example:

```
backup MyBackupFileName repository MyRepo application NCS
```

If you want to use this repository for automatic backups, see [Specify the Backup Repository for Automatic Backups, on page 624](#).

## Use Remote SFTP Backup Repositories



**Note** We recommend using remote NFS repositories.

You can create backup repositories on a remote SFTP server and configure the Cisco EPN Manager server to use them.

The SFTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Cisco EPN Manager server.
- Has a user with write access to the SFTP server disk.
- Has a local shared folder where the backups will be stored.

Other than these requirements, no other configuration is needed on the SFTP backup server.

For the SFTP server details to appear in the **Backup Repository** drop-down list in the web GUI, you should configure the SFTP server using the CLI. You can configure the SFTP server only using the CLI.

**Step 1** Log into the server as the Cisco EPN Manager CLI admin user. See [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).

**Step 2** Enter configuration mode:

```
configure terminal
config#
```

**Step 3** Configure a symbolic link to the remote SFTP server, then exit configuration mode:

```
config# repository repositoryName
config-Repository# url sftp://RemoteServerIP//sharedFolder
config-Repository# user userName password plain userPassword
config-Repository# exit
config# exit
```

Where:

- *repositoryName* is the name of the repository (for example, **MyRepo** or **EPNManager**).

- *RemoteServerIP* is the IP address of the SFTP server hosting the shared backup folder. Note that the example above specifies an absolute path to the shared folder. To specify a relative path to the shared folder, use only one slash in the URL (for example, **url sftp://RemoteServerIP/sharedfolder**).
- *sharedFolder* is the name of the shared backup folder on the SFTP server.
- *userName* is the name of the user with write privileges to the repository on the SFTP server.
- *userPassword* is the corresponding password for that user.

**Step 4** Verify the creation of the symbolic link:

```
show repository repositoryName
```

---

### What to do next

When you perform a manual backup, specify the new repository as the repository name in the backup command. For example:

```
backup MyBackupFileName repository MyRepo application NCS
```

If you want to use this repository for automatic backups, see [Specify the Backup Repository for Automatic Backups, on page 624](#).

## Delete a Local Backup Repository

Use the following procedure to delete a local backup repository. This procedure ensures that the admin interface has the updated information.

- 
- Step 1** Log into the server as a Cisco EPN Manager CLI admin user (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)).
- Step 2** List the local application backup repositories and identify the one that you want to delete:
- ```
show running-config | begin repository
```
- Step 3** Enter configuration mode and delete the repository:
- ```
configure terminal
(config)# no repository repositoryName
```
- Step 4** Repeat step 2 to verify that the repository was deleted.
- 

## Set Up Automatic Application Backups

Automatic application backups are enabled by default after installation. You can customize the schedule, specify a different backup repository, or adjust the number of backups that are saved.

To check what data is saved by the backup mechanism (and verify whether you need to manually save any data that is not backed up), see these topics:

- [Information That Is Backed Up, on page 616](#)
- [Information That Is Not Backed Up, on page 618](#)

## Schedule Automatic Application Backups

Automatic application backups are enabled by default but you can adjust the day and interval at which these backups are performed. Performing a backup is resource-intensive and affects Cisco EPN Manager server performance. Avoid scheduling automatic backups to occur at peak traffic times.

If an automatic application backup fails, Cisco EPN Manager generates a Backup Failure alarm (with major severity). You can view these alarms just as you do other alarms (see [Find and View Alarms, on page 221](#)). You can also get email notifications for these alarms if you include the System alarm category in your email notification settings (see [Forward Alarms and Events as Email Notifications, on page 229](#)).



**Note** After an automatic application backup fails, a pop-up message is displayed before every subsequent login attempt. This message will continue to appear until you acknowledge the corresponding alarm.

- 
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
  - Step 2** Choose **System Jobs > Infrastructure**.
  - Step 3** In the Jobs list, check the **Server Backup** check box, then click **Edit Schedule**. The Schedule dialog box opens.
  - Step 4** In the Schedule dialog box, select a start date, recurrence interval, and optional end time.
  - Step 5** Click **Submit**. These settings will now be used for future automatic application backups.
- 

## Specify the Backup Repository for Automatic Backups

You can use the Cisco EPN Manager interface to specify a different backup repository for automatic application backups. The backup repository can be local or remote. You can also use the interface to create a new local backup repository if it does not already exist.

### Before you begin

If you want to use a remote repository for automatic backups, you must create the repository first. Only local repositories can be created using this procedure. See [Set Up and Manage Repositories, on page 618](#).

- 
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
  - Step 2** Choose **System Jobs > Infrastructure**.
  - Step 3** In the list of jobs, check the **Server Backup** check box.
  - Step 4** Click **Edit** (the pencil icon). The Edit Job Properties dialog box opens.
  - Step 5** Select a repository from the Backup Repository drop-down list, then click **Save**. Cisco EPN Manager will use the new repository when it performs the next automatic application backup.
-

## Change the Number of Automatic Application Backups That Are Saved

Follow this procedure to adjust the number of automatic application backups that are saved on a local repository. When a backup exceeds the number you specify here, Cisco EPN Manager deletes the oldest backup from the repository.

The **Max UI backups to keep** setting does not apply if you are using remote repositories for automatic application backups. You must monitor and archive or delete old backups on remote repositories using your own methods.

- 
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
  - Step 2** Choose **System Jobs > Infrastructure**.
  - Step 3** In the Jobs list, check the **Server Backup** check box.
  - Step 4** Click **Edit** (the pencil icon) to open the Edit Job Properties dialog box.
  - Step 5** Enter a value in the **Max UI backups to keep** field, then click **Save**. Cisco EPN Manager will enforce this setting at the next backup.
- 

## Perform a Manual Backup

The topics in this section explain how to perform manual application or appliance backups.

To check what data is saved by the backup mechanism (and verify whether you need to manually save any data that is not backed up), see these topics:

- [Information That Is Backed Up, on page 616](#)
- [Information That Is Not Backed Up, on page 618](#)

## Perform an Immediate Application Backup

Cisco EPN Manager performs automatic application backups as described in [Backup Scheduling, on page 614](#). If needed, you can manually trigger an application backup as described in the following topics.

### Perform an Immediate Application Backup Using the Web GUI

Use this procedure to trigger an immediate application backup using the web GUI.

- 
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
  - Step 2** Choose **System Jobs > Infrastructure**.
  - Step 3** In the Jobs list, check the **Server Backup** check box, then click **Run**.
  - Step 4** To view the backup status, scroll to the top of the table to locate the new job, then check its status and results.
-

## Perform an Immediate Application Backup Using the CLI

Use this procedure to trigger an immediate application backup using the CLI.

- 
- Step 1** Log into the server as a Cisco EPN Manager CLI admin user (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)).
- Step 2** Display the list of backups, where *repositoryName* is the backup repository:
- ```
show repository repositoryName
```
- Step 3** Start the remote backup.
- ```
backup filename repository repositoryName application NCS
```
- where *filename* is the name that you want to give the appliance backup file (for example, myBackup). The character length of the file name is 26. Other information is appended to the filename automatically, as explained in [Backup Filenames, on page 615](#)
- 

## Perform a Manual Appliance Backup

Use this procedure to perform an appliance backup to a remote repository. Be sure you have configured the remote repository as described in [Set Up NFS-Based Remote Repositories, on page 620](#).

- 
- Step 1** Make sure the remote host is available.
- Step 2** Log into the Cisco EPN Manager server as admin (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)).
- Step 3** Start the remote backup:
- ```
(admin) # backup filename repository repositoryName
```
- Step 4** To verify that the backup transfer is complete, view the md5Checksum and file size.
- 

## Restore Cisco EPN Manager Data

All restore operations are performed using the CLI. Data can be restored to the host where the backup is executed (local host), or to a remote host. Backups can only be restored in their entirety; you cannot restore only parts of a backup.

See these topics for more information:

- [Restore an Application Backup, on page 627](#)
- [Restore an Appliance Backup, on page 627](#)



## Restore an Application Backup



**Note** To restore an *appliance* backup, use the procedure in [Restore an Appliance Backup, on page 627](#).

When you restore an application backup, make sure it is being restored to an OVA installation of the same size or larger. If the OVA installation is smaller, the restore will fail.

### Before you begin

If you are using high availability, read the guidelines in [Restore Data In an HA Deployment, on page 732](#) before restoring your data.

- 
- Step 1** Log into the server as a Cisco EPN Manager CLI admin user (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)).
- Step 2** If a previous restoration attempt failed, the database may have been corrupted. Run this command to recreate the database:
- ```
ncs run reset db
```
- Step 3** List the saved application backups and identify the one that you want to restore. *repositoryName* is the repository that contains the backup files.
- ```
show repository repositoryName
```
- Step 4** From the vmWare vSphere client (OVA) or the Cisco IMC server (Bare Metal), restore the data:
- ```
restore backupFileName repository repositoryName application NCS
```
- Step 5** If you are using Cisco Smart Licensing, re-register Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. See [Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 589](#).
- 

## Restore an Appliance Backup



**Note** To restore an *application* backup, use the procedure in [Restore an Application Backup, on page 627](#).

When you restore an appliance backup, make sure it is being restored to an OVA installation of the same size or larger. If the OVA installation is smaller, the restore will fail.

Cisco recommends that you change the restored server's IP address, subnet mask, and default gateway if:

- The restored host is on the same subnet as the old host, and the old host is still active.
- The restored host is on a different subnet from the old host.

### Before you begin

If you are using high availability, read the information in [Restore Data In an HA Deployment, on page 732](#) before restoring your data.

- 
- Step 1** Log into the server as a Cisco EPN Manager CLI admin user (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)).
- Step 2** If a previous restoration attempt failed, the database may have been corrupted. With the backup stored in an external repository, reinstall the setup using the same release and then retry the restore.
- Step 3** List the saved appliance backups and identify the one that you want to restore. *repositoryName* is the repository that contains the backup files.
- ```
show repository repositoryName
```
- Step 4** From the vmWare vSphere client (OVA) or the Cisco IMC server (Bare Metal), restore the data:
- ```
restore backupFileName repository repositoryName
```
- Step 5** Determine whether you should change the IP address, subnet mask, and default gateway.
- Check if your installation meets the following criteria:
    - The restored host is on the same subnet as the old host, and the old host is still active.
    - The restored host is on a different subnet from the old host.
 If it does, perform the next step.
  - Change the IP address, subnet mask, default gateway and (optionally) the host name on the restored server.
  - Write the changes to the server's running configuration and restart Cisco EPN Manager services. For example:
- ```
configure terminal
(config)# int GigabitEthernet 0
(config-GigabitEthernet)# ip address IPAddress subnetMask
(config-GigabitEthernet)# exit
(config)# ip default-gateway gatewayIP
(config)# hostname hostname
(config)# exit
(admin)# write mem
(admin)# ncs stop
(admin)# ncs start
(admin)# exit
```
- Step 6** If you are using Cisco Smart Licensing, re-register Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. See [Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 589](#).
- 

## Recover from Failed Restores

You may sometimes find that a restore does not complete, or reports a failure. Whenever a restore fails, you run the risk of database corruption, which can prevent the further restoration or re-installation. Perform the following steps to restore a corrupted database before attempting another restore or re-installation.

- 
- Step 1** Open a CLI session with the Cisco EPN Manager server (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)).
- Step 2** Enter the following command to reset the corrupted database:
- ```
ncs run reset db
```
-

# Manage Disk Space Issues During Backup and Restore

If you are experiencing disk issues *during* a backup or restore, move your installation to a server with adequate disk space by following the procedure in [Migrate to Another Virtual Appliance Using Backup and Restore, on page 629](#).

If you are unable to create a backup *after* a restore of your existing system, follow the steps explained in [Compact the Database, on page 651](#) to free disk space and create a successful backup. If you are still unable to create a backup after using the `ncs cleanup` command, set up and use a remote repository (using NFS, FTP, or SFTP) for your backups, as explained in [Use a Remote Backup Repository, on page 619](#).

# Migrate to Another Virtual Appliance Using Backup and Restore

You will need to migrate your Cisco EPN Manager data from an existing virtual appliance (OVA server installation) to a new one whenever you want to:

- Replace the old server entirely, such as after a catastrophic hardware failure. In this case, you can use your old installation media to re-create the new host on a replacement server, then migrate your application data from the old host to the new host.
- Migrate to a larger or more powerful server, so you can use Cisco EPN Manager to manage more of your network. In this case, you will want to ensure that you have the OVA installation file and install it on the new server using the larger installation option before retiring the older, smaller one. You can then migrate your application data from the old host.

In both cases, it is relatively easy to migrate your old data to the new virtual appliance by restoring to the new host an appliance or application backup taken from the old host.

- 
- |               |                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | If you have not already done so, set up a remote backup repository for the old host, as explained in <a href="#">Use a Remote Backup Repository, on page 619</a> .            |
| <b>Step 2</b> | Perform an application backup of the old host and save it to the remote repository (see <a href="#">Perform an Immediate Application Backup Using the CLI, on page 626</a> ). |
| <b>Step 3</b> | Install the new host (installation steps are in the <a href="#">Cisco Evolved Programmable Network Manager Installation Guide</a> ).                                          |
| <b>Step 4</b> | Configure the new host to use the same remote backup repository as the old host (see <a href="#">Use a Remote Backup Repository, on page 619</a> ).                           |
| <b>Step 5</b> | Restore the application backup on the remote repository to the new host (see <a href="#">Restore an Application Backup, on page 627</a> ).                                    |
-





## CHAPTER 23

# Server Health and Configuration

---

- [View the Cisco EPN Manager Server Configuration](#), on page 631
- [Change the Cisco EPN Manager Hostname](#), on page 632
- [Secure the Connectivity of the Cisco EPN Manager Server](#), on page 633
- [Establish an SSH Session With the Cisco EPN Manager Server](#), on page 644
- [Set Up NTP on the Server](#), on page 644
- [Set Up the Cisco EPN Manager Proxy Server](#), on page 645
- [Set Up the SMTP E-Mail Server](#), on page 645
- [Enable FTP/TFTP/SFTP Service on the Server](#), on page 646
- [Configure Stored Cisco.com Credentials](#), on page 646
- [Create a Login Banner \(Login Disclaimer\)](#), on page 647
- [Stop and Restart Cisco EPN Manager](#), on page 647
- [Configure Global SNMP Settings for Communication with Network Elements](#), on page 647
- [Manage Administrative Passwords](#), on page 648
- [Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard](#), on page 650
- [Improve the Cisco EPN Manager Server Performance](#), on page 651
- [Work With Server Internal SNMP Traps That Indicate System Problems](#), on page 652
- [Set Up Defaults for Cisco Support Requests](#), on page 654
- [Configure Cisco Product Feedback Settings](#), on page 654

## View the Cisco EPN Manager Server Configuration

Use this procedure to view Cisco EPN Manager server configuration information such as the current server time, kernel version, operating system, hardware information, and so forth.

- 
- |               |                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Administration &gt; Dashboards &gt; System Monitoring Dashboard</b> .                          |
| <b>Step 2</b> | Click the <b>Overview</b> tab.                                                                           |
| <b>Step 3</b> | Click <b>System Information</b> at the top left of the dashboard to expand the System Information field. |
-

# Change the Cisco EPN Manager Hostname

Cisco EPN Manager prompts you to enter a hostname when you install the server. For a variety of reasons, you may find a mismatch between the hostname configured on the Cisco EPN Manager server and the hostname configured elsewhere. You can resolve this issue without reinstalling Cisco EPN Manager by changing its hostname on the server. To do so:

- 
- Step 1** Open a CLI session with the Cisco EPN Manager server, making sure you enter **configure terminal** mode.  
See [Connect via CLI](#).
- Step 2** Enter the following command:
- ```
Cisco_EPN_Manager_Server/admin(config)#hostname newHostName
```
- where *newHostName* is the hostname you want to assign to the Cisco EPN Manager server.
- Step 3** Restart the Cisco EPN Manager server using the **ncs stop** and **ncs start** commands.
- Step 4** Check the hostname configured for your SSL server certificate:
- If the hostname is the same as the one you specified in Step 2, you can stop here.
  - If the hostname is different, you will need to create a new SSL server certificate configured with the hostname you specified in Step 2 and then install it. See [Set Up HTTPS to Secure the Connectivity of the Web Server](#).
- 

## Connect via CLI

Administrators can connect to the Cisco EPN Manager server via its command-line interface (CLI). CLI access is required when you need to run commands and processes accessible only via the Cisco EPN Manager CLI. These include commands to start the server, stop it, check on its status, and so on.

### Before you begin

Before you begin, make sure you:

- Know the user ID and password of an administrative user with CLI access to that server or appliance. Unless specifically barred from doing so, all administrative users have CLI access.
- Know the IP address or host name of the Cisco EPN Manager server.

- 
- Step 1** Start up your SSH client, start an SSH session via your local machine's command line, or connect to the dedicated console on the Cisco EPN Manager physical or virtual appliance.
- Step 2** Log in as appropriate: If you are using a GUI client: Enter the ID of an active administrator with CLI access and the IP address or host name of the Cisco EPN Manager server. Then initiate the connection. If you are using a command-line client or session: Log in with a command like the following: `[localhost]# ssh username@IPHost` -Where *username* is the user ID of a Cisco EPN Manager administrator with CLI access to the server. *IPHost* is the IP address or host name of the Cisco EPN Manager server or appliance. If you are using the console: A prompt is shown for the administrator user name. Enter the user name.

Cisco EPN Manager will then prompt you for the password for the administrator ID you entered.

**Step 3** Enter the administrative ID password. Cisco EPN Manager will present a command prompt like the following:

```
Cisco_EPN_Manager_Server/admin#
```

**Step 4** If the command you need to enter requires that you enter **configure terminal** mode, enter the following command at the prompt:

```
Cisco_EPN_Manager_Server/admin#configure terminal
```

The prompt will change from `Cisco_EPN_Manager_Server/admin#` to `Cisco_EPN_Manager_Server/admin/conf#`.

---

## Secure the Connectivity of the Cisco EPN Manager Server

For data security, Cisco EPN Manager encrypts data in transit using standard public key cryptography methods and public key infrastructure (PKI). You can obtain more information about these technologies from the internet. Cisco EPN Manager encrypts the data that is exchanged between the following connections:

- Between the web server and the web client
- Between a CLI client and the Cisco EPN Manager CLI shell interface (handled by SSH)
- Between the Cisco EPN Manager and systems such as AAA and external storage

To secure communication between the web server and web client, use the public key cryptography services that are built in as part of the HTTPS mechanism. For that you need to generate a public key for the Cisco EPN Manager web server, store it on the server, and then share it with the web client. This can be done using the standard PKI certificate mechanism which not only shares the web server public key with the web client, but also guarantees that the public key belongs to the web server (URL) you are accessing. This prevents any third party from posing as the web server and collecting sensitive information that the web client is sending to the web server. Follow the procedure in [Set Up HTTPS to Secure the Connectivity of the Web Server, on page 633](#)

These topics provide additional steps you can take to secure the web server:

- Cisco recommends that the Cisco EPN Manager web server authenticate web clients using certificate-based authentication. This security hardening procedure is described in [Set Up Certificate-Based Authentication for Web Clients, on page 746](#)
- To secure connectivity between a CLI client and the Cisco EPN Manager CLI interface, refer to the security hardening procedures in [Harden the Cisco EPN Manager Server, on page 749](#).
- To secure connectivity between the Cisco EPN Manager and systems such as AAA and external storage, refer to the recommendations in [Harden Your Cisco EPN Manager Storage, on page 751](#).

## Set Up HTTPS to Secure the Connectivity of the Web Server

HTTPS operations use a server key that is generated using public key cryptography algorithms, and trust chain certificates that are generated using the server key. These certificates are applied to the Cisco EPN Manager web server. Depending upon how you generated the certificates, you may have to request the client browsers to trust these certificates the first time the browser connects to the web server. The HTTPS mechanism ensures the security of the server machine (which in turn improves security of all other associated systems).

Use one of the following two methods to generate and install the web server certificate (do not use the methods together).

| Signing Entity                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | See:                                                                               |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Self-signed certificates                       | <p>You generate the self-signed certificates and then apply them to the web server. This method can be used on:</p> <ul style="list-style-type: none"> <li>• Deployments that do not use HA</li> <li>• HA deployments that <i>do not</i> use virtual IP addresses.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <a href="#">Generate and Apply Self-Signed Web Server Certificate, on page 634</a> |
| Certificate Authority (CA) signed certificates | <p>A Certificate Authority (CA) generates and issues these certificates. The certificates bind a public key to the name of the entity (for example, a server or device) that is identified in the certificate. You must generate a Certificate Signing Request (CSR) file from the Cisco EPN Manager server, and submit the CSR file (which contains the server key) to the CA. When you receive the certificates, you apply them to the web server.</p> <p>These certificates can be generated by an external CA or an internal CA.</p> <ul style="list-style-type: none"> <li>• External CA—An external CA organization validates identities and issues the certificates, usually for a fee. (Popular browsers are usually pre-installed with Root and Intermediate certificates issued by the external CA organization).</li> <li>• Internal CA—Uses a certificate-generating server within your organization (this avoids a fee). The internal CA functions exactly the same way as an external fee-based CA.</li> </ul> <p>This method can be used on:</p> <ul style="list-style-type: none"> <li>• Deployments that do not use HA</li> <li>• HA deployments that <i>do</i> use virtual IP addresses (including SSL connections between browser-based clients)</li> </ul> <p><b>Note</b> Depending on your deployment, you may need to instruct your users to install the CA-signed Root and Intermediate certificates to their browser or OS certificate store. Ask your organization's IT administrator if this is required. Instructions are provided in <a href="#">Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 642</a>.</p> | <a href="#">Generate and Apply a CA-Signed Web Server Certificate, on page 635</a> |

## Generate and Apply Self-Signed Web Server Certificate

The following procedure generates an RSA key and then applies a self-signed certificate with domain information.

### Before you begin

Make sure you have the fully qualified domain name (FQDN) of the server. You will need it for this procedure.



- 
- Step 1** Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.
- Step 2** Enter the following command:
- ```
ncs key genkey -newdn
```
- Step 3** To activate the certificate, restart Cisco EPN Manager . See [Stop and Restart Cisco EPN Manager](#) , on page 647.
- 

## Generate and Apply a CA-Signed Web Server Certificate

The following topics explain how to generate and apply CA-signed certificates to the Cisco EPN Manager web server. The procedures are slightly different depending on whether or not your deployment is using HA, and if it is using HA, whether or not you are using HA with virtual IP addresses.

You may need to instruct your users to install the Root and Intermediate CA certificates to their browser or OS certificate store. Ask your organization's IT administrator if this is required. Instructions are provided in [Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store](#), on page 642.

Deployment Type	Summary of Steps
Deployment without HA	<p>For deployments without HA, you must request the certificate, import it into your web server, and restart the web server to apply it, as described in these topics:</p> <ol style="list-style-type: none"> <li>1. <a href="#">Request a CA-Signed Web Server Certificate</a>, on page 635</li> <li>2. <a href="#">Import and Apply a CA-Signed Web Server Certificate—No HA</a>, on page 637</li> </ol>
High availability deployment <i>not using</i> virtual IP addresses	<p>For HA deployments that do not use virtual IPs, you must request separate certificates for the primary and secondary servers and then import the appropriate certificate onto each server. When you restart the servers to apply the certificates, you must restart them in a specific order. The entire procedure is described in these topics:</p> <ol style="list-style-type: none"> <li>1. <a href="#">Request a CA-Signed Web Server Certificate</a>, on page 635</li> <li>2. <a href="#">Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses</a>, on page 638</li> </ol>
High availability deployment <i>using</i> virtual IP addresses	<p>For HA deployments that use virtual IPs, you only need to request a single certificate for both servers. You must remove HA on the servers, import the certificate on both servers, and then restart the servers to apply the certificate (you must restart the servers in a specific order). Finally, you reconfigure HA by registering the secondary server on the primary server. The entire procedure is described in these topics:</p> <ol style="list-style-type: none"> <li>1. <a href="#">Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses</a>, on page 640</li> <li>2. <a href="#">Register the Secondary Server on the Primary Server</a>, on page 729</li> </ol>

### Request a CA-Signed Web Server Certificate

Use this procedure to request a CA-signed web server certificate for your deployment. You should use this procedure if:

- Your deployment does not use HA
- Your deployment uses HA but does not use virtual IP addressing (you will need to perform the following procedure on both servers)



**Note** If your deployment uses HA with virtual IP addresses, use the procedure in [Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses, on page 640](#).

### Before you begin

Make sure SCP is enabled on your machine and all relevant ports are open. This is required so that you can copy files to and from the server.

- Step 1** Generate a Certificate Signing Request (CSR) file for the Cisco EPN Manager server:
- Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.
  - Enter the following command to generate the CSR file in the default backup repository (defaultRepo):

```
ncs key genkey -newdn -csr CertName.csr repository defaultRepo
```

where *CertName* is an arbitrary name of your choice.

- Step 2** Copy the CSR file from the Cisco EPN Manager server to your local machine.
- Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.
  - Log in as the Linux CLI root user. See [Log In and Out as the Linux CLI root User, on page 670](#).
  - Copy the file from the Cisco EPN Manager server to your local machine. For example:

```
scp /localdisk/defaultRepo/CertName.csr clientUserName@clientIP:/destinationFolder
```

- Log out as the Linux CLI root user.

- Step 3** Submit the CSR file to a Certificate Authority of your choice.

**Note** Once you have generated and sent the CSR file for certification, do *not* use the **genkey** command to generate a new key on the same Cisco EPN Manager server. If you do, when you try to import the signed certificate file, you will receive an error due to a mismatch between keys in the file and on the Cisco EPN Manager server.

The CA will send you digitally-signed certificates either in a single file with the name *CertFilename.cer*, or as a set of multiple files.

- Step 4** (HA deployments not using virtual IP addresses) Repeat these steps for the secondary server.

### What to do next

When you receive the certificates from the CA, import and apply the certificates. Use one of the following procedures, depending on your deployment:

- [Import and Apply a CA-Signed Web Server Certificate—No HA, on page 637](#)
- [Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses, on page 638](#)

## Import and Apply a CA-Signed Web Server Certificate—No HA

This topic explains how to import and apply CA-signed web server certificates to a deployment that does not use HA.

### Before you begin

- You must have the CA-signed certificates you requested using [Request a CA-Signed Web Server Certificate, on page 635](#). You cannot perform the following procedure until you have received the certificates.
- Make sure SCP is enabled on your local machine and all relevant ports are open. This is required so that you can copy files to and from the server.

### Step 1

If you receive only one CER file from the CA, proceed to Step 2. If you receive multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

- Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```
-----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-----
```

- Save this new file with a new name in the format *CertFilename.cer*.

### Step 2

Copy the CER file from your local machine to the backup repository on the Cisco EPN Manager server.

- Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.
- Log in as the Linux CLI root user. See [Log In and Out as the Linux CLI root User, on page 670](#).
- Retrieve the file from your local machine and copy it to the Cisco EPN Manager server default backup repository (defaultRepo):

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

- Log out as the Linux CLI root user.

### Step 3

As the Cisco EPN Manager CLI admin user, import the CER file.

```
ncs key importsigndcert CertFilename.cer repository RepoName
```

### Step 4

Restart Cisco EPN Manager to activate this certificate. See [Stop and Restart Cisco EPN Manager, on page 647](#).

### What to do next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See [Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 642](#) for more information.

## Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses

This topic explains how to import and apply CA-signed web server certificates to an HA deployment that is *not* using virtual IP addresses. (If you have an HA deployment that *does* use virtual IPs, see [Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses, on page 640](#).) This procedure is similar to the procedure for a deployment that does have HA, except that you have to perform the procedure on both the primary server and the secondary server.



**Note** When you restart the servers, follow these steps carefully because the servers must be restarted in a specific sequence.

### Before you begin

- You must have the CA-signed certificates you requested using [Request a CA-Signed Web Server Certificate, on page 635](#). You cannot perform the following procedure until you have received the certificates for each server.
- Make sure SCP is enabled on your local machine and all relevant ports are open. This is required so that you can copy files to and from the server.

**Step 1** Import the primary certificates onto the primary server.

- If you received only one CER file from the CA, proceed to Step 1(b). If you received multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.
- Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```
-----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-----
```

- Save this new file with a new name in the format *CertFilename.cer*.

- Log in to the primary Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.
- Log in as the Linux CLI root user. See [Log In and Out as the Linux CLI root User, on page 670](#).
- Retrieve the CER file from your local machine and copy it to the Cisco EPN Manager server's default backup repository (defaultRepo):

```
scp clientUserName@clientIP:/fullPathToCERfile /localdisk/defaultRepo
```

- Log out as the Linux CLI root user.

**Step 2** Perform the previous step on the secondary server.

**Step 3** On the *secondary* server, import the CER file.

- a) Log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

- b) Verify that the secondary server is stopped.  
c) Import the CER file:

```
ncs key importsigndcert CertFilename.cer repository RepoName
```

**Note** Do not restart the secondary server until you reach Step 5.

**Step 4** On the *primary* server, import the CER file.

- a) Log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

- b) Verify that the primary server is stopped.  
c) Import the CER file:

```
ncs key importsigndcert CertFilename.cer repository RepoName
```

**Note** Do not restart the primary server until you reach Step 6.

**Step 5** On the *secondary* server, run the following commands:

- a) Run the **ncs start** command to restart the server.  
b) Verify that the secondary server has restarted.  
c) Run the **ncs status** command and verify that the HA status of the secondary server is **Secondary Lost Primary**.

**Step 6** On the *primary* server, run the following commands:

- a) Run the **ncs start** command to restart the server.  
b) Verify that the primary server has restarted.  
c) Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted.

Once all the processes on the primary server are up and running, HA registration is automatically triggered between the secondary and primary servers (and an email is sent to the registered email addresses). This normally completes after a few minutes.

**Step 7** Verify the HA status on the primary and secondary servers by running the **ncs ha status** command on both servers. You should see the following:

- The primary server state is **Primary Active**.
- The secondary server state is **Secondary Syncing**.

---

### What to do next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See [Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 642](#) for more information.

## Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses

If you have a high availability deployment that uses virtual IP addresses, you need to make only one certificate request. When you receive the certificate from the CA, you install the same certificate on both the primary and secondary servers. This is different from HA deployments that do not use IP addressing, where you make two certificate requests and install one certificate on the primary server and the other (different) certificate on the secondary server.

For more information on virtual IPs and HA, see [Using Virtual IP Addressing With HA, on page 728](#)

### Before you begin

Make sure SCP is enabled on your machine and all relevant ports are open. This is required so that you can copy files to and from the server.

### Step 1

Generate a CSR file and private key for the primary and secondary servers. You will install the private key on both servers, and submit the CSR file to a Certificate Authority of your choice. The following example shows how to create these files using openssl in Linux.

- a) Generate the CSR file in the default backup repository.

```
openssl req -newkey rsa:2048 -nodes -keyout ServerKeyFileName -out CSRFileName -config
opensslCSRconfigFileName
```

where:

- *ServerKeyFileName* is the name you want to use for the private key file.
- *CSRFileName* is the name that you want to use for the CSR request file, which will be submitted to the CA.
- *opensslCSRconfigFileName* is the name of the file that contains the openssl configurations used to generate the CSR file.

- b) Using a text editor, edit the file with openssl configurations (*opensslCSRconfigFileName* in (a)) to have contents similar to the following.

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req

[req_distinguished_name]
countryName = Country
countryName_default = US
stateOrProvinceName = State
stateOrProvinceName_default = CA
localityName = City
localityName_default = San Jose
organizationName = Organization
organizationName_default = Cisco Systems
organizationalUnitName = Organizational Unit
organizationalUnitName_default = CSG
commonName = Common Name
commonName_default = example.cisco.com
commonName_max = 64

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
```

```

DNS.1 = example.cisco.com
DNS.2 = example-pri.cisco.com
DNS.3 = example-sec.cisco.com
IP.1 = 209.165.200.224
IP.2 = 209.165.200.225
IP.3 = 209.165.200.226

```

In this example:

- The virtual IP address is 209.165.200.224. The FQDN for is **example.cisco.com**. The FQDN is also used for the DNS server name.
- The primary server IP address is 209.165.200.225. Its hostname is **example-pri**. This hostname should be included in /etc/hosts and other hostname setting files.
- The secondary server IP address is 209.165.200.226. Its hostname is **example-sec**.

**Step 2** Submit the CSR file to a Certificate Authority of your choice. The CA will send you digitally-signed certificates either in a single file with the name *CertFilename.cer*, or as a set of multiple files.

**Step 3** If you receive only one CER file from the CA, proceed to Step 4. If you receive multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

- a) Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```

-----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-----

```

- b) Save this new file with a new name in the format *CertFilename.cer*.

**Step 4** On the primary server, copy the CER file to the backup repository on each server.

- a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.  
b) Log in as the Linux CLI root user. See [Log In and Out as the Linux CLI root User, on page 670](#).  
c) Retrieve the file from your local machine and copy it to the server's default backup repository (defaultRepo).

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

- d) Log out as the Linux CLI root user.

**Step 5** Repeat the previous step on the secondary server.

**Step 6** On the *primary* server, as the Cisco EPN Manager CLI admin user, remove the HA settings:

```
ncs ha remove
```

Run the **ncs ha status** to verify if the HA settings is removed before proceeding with the next step.

**Step 7** On both the primary and secondary server, import the CER file.

```
ncs key importsigndcert CertFilename.cer repository RepoName
```

**Step 8** Restart the primary and secondary servers. Because they are not yet paired for HA, the order does not matter. See [Stop and Restart Cisco EPN Manager](#) , on page 647.

**Note** If the server does not restart, it may indicate that you mistakenly imported an individual certificate file instead of a concatenated certificate file (even though the import operation appeared to be successful). To fix this, repeat the import operation using the (correct) concatenated certificate file.

**Step 9** Verify the status of the primary and secondary servers by running the **ncs status** command on both servers.

**Step 10** Register the secondary server on the primary server for HA. See [Register the Secondary Server on the Primary Server](#), on page 729.

### What to do next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See [Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store](#), on page 642 for more information.

### Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store

Ask your organization's IT administrator if your users should install the CA Root and Intermediate CA certificates to their browser or OS certificate store. If not done in situations where it is required, users will see indications on their browsers that the browsers are not trusted.

Depending on your browser type and version, the exact steps for this procedure may be slightly different.

### Before you begin

If you are adding the certificates to an Internet Explorer browser, you must have Administrator privileges on your client machine.

**Step 1** For Firefox browsers, follow these steps to import the certificates.

- a) Choose **Tools > Options**, then click **Advanced** from the options on the left.
- b) Click **Certificates** from the list at the top of the window, then click **View Certificates**. This opens the browser's Certificate Manager dialog box.
- c) In the Certificate Manager dialog box, click the **Authorities** tab, then click **Import** at the bottom of the dialog box.
- d) In the **Select File...** dialog box, browse to the CA-signed Root certificate file, then click **Open**.
- e) Import the file.
- f) Repeat the import steps for the CA-signed Intermediate certificate file.

**Step 2** For Internet Explorer browsers, use the Microsoft Certificate Manager tool to import the certificates. To use this tool, users must have Administrator privileges on their client machine.

- a) In Windows 7, click **Start**.
- b) Enter **certmgr.msc** in the Search text box, then hit Return.
- c) Launch the Microsoft Certificate Manager by clicking the program's icon in the Search results.
- d) In the left column of the Certificate Manager GUI, choose **Trusted Root Certification Authorities**.
- e) Left-click **Certificates**, then choose **All Tasks > Import**.
- f) Click **Next**, then browse to the CA-signed Root certificate file, and import it.



- g) Repeat the import steps for the CA-signed Intermediate certificate file, but choose **Intermediate Certification Authorities** as the first step for importing the certificate.

---

## Change the HTTPS Server Port

Because many devices use HTTPS to relay device configuration information, HTTPS is enabled by default in Cisco EPN Manager . (HTTP is not used by Cisco EPN Manager and is disabled by default.) If needed, you can change the port for the HTTPS server by following these steps.

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Server**.
- Step 2** In the HTTPS area, enter the new port number, then click **Save**.
- Step 3** Restart Cisco EPN Manager to apply your changes. See [Stop and Restart Cisco EPN Manager](#) , on page 647.
- 

## View Existing CA Certificates

To view existing certificates for the Cisco EPN Manager server:

- 
- Step 1** Log in to the Cisco EPN Manager Admin CLI as the admin user.
- Step 2** To view the list of CA certificates that exist in the Cisco EPN Manager trust store, enter the following command:
- ```
ncs key listcacerts
```
- Step 3** To see the complete trust chain for SSL/HTTPS operations, log in to the Cisco EPN Manager web GUI using Google Chrome, and use Chrome to view the CA-signed certificate that the server sent to the browser. Chrome will display all the linked certificates in the trust chain.
- 

## Delete CA Certificates

- 
- Step 1** Log in to the Cisco EPN Manager server as the admin user.
- Step 2** Because you will need the certificate short names for the delete command, list the short names of all the CA certificates on the Cisco EPN Manager server:
- ```
ncs key listcacert
```
- Step 3** Locate the CA certificate you want to delete and enter the following command:
- ```
ncs key deletecacert aliasname
```

where *aliasname* is the short name of the CA certificate you want to delete.

---

# Establish an SSH Session With the Cisco EPN Manager Server

When you connect to the server, use SSH and log in as the admin user. (See [User Interfaces, User Types, and How To Transition Between Them, on page 667](#) for more information.)

**Step 1** Start your SSH session and log in as the Cisco EPN Manager admin user.

- From the command line, enter the following, where *server-ip* is the Cisco EPN Manager :

```
ssh admin server-ip
```

- Open an SSH client and log in as **admin**.

**Step 2** Enter the admin password. The prompt will change to the following:

```
(admin)
```

To view a list of the operations the admin user can perform, enter **?** at the prompt.

To enter admin config mode, enter the following command (note the change in the prompt):

```
(admin) configure terminal
(config)
```

## Set Up NTP on the Server

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the Cisco EPN Manager server. Failure to manage NTP synchronizations across your network can result in anomalous results in Cisco EPN Manager . This includes all Cisco EPN Manager -related servers: Any remote FTP servers that you use for Cisco EPN Manager backups, secondary Cisco EPN Manager high-availability servers, and so on.

You specify the default and secondary NTP servers during Cisco EPN Manager server installation. You can also use Cisco EPN Manager 's **ntp server** command to add to or change the list of NTP servers after installation.



**Note**

Cisco EPN Manager cannot be configured as an NTP server; it acts as an NTP client only. Up to three NTP servers are allowed.

**Step 1** Log in to the Cisco EPN Manager server as the admin user and enter config mode. See [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).

**Step 2** Set up the NTP server using one of the following commands.

```
ntp server ntp-server-IP ntp-key-id ntp-key
```

Where:

- *ntp-server-IP* is the IP address or hostname of the server providing the clock synchronization to the Cisco EPN Manager server
- *ntp-key-id ntp-key* is the md5 key ID md5 key of the authenticated NTP server

---

## Set Up the Cisco EPN Manager Proxy Server

Use this procedure to configure proxies for the server and, if configured, its local authentication server. If you use a proxy server as a security barrier between your network and the Internet, you need to configure the proxy settings as shown in the following steps:

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Account Settings**.
  - Step 2** Click the **Proxy** tab.
  - Step 3** Select the **Enable Proxy** check box and enter the required information about the server that has connectivity to Cisco.com and will act as the proxy.
  - Step 4** Select the **Authentication Proxy** check box and enter the proxy server's user name and password.
  - Step 5** Click **Test Connectivity** to check the connection to the proxy server.
  - Step 6** Click **Save**.
- 

## Set Up the SMTP E-Mail Server

To enable Cisco EPN Manager to send email notifications (for alarms, jobs, reports, and so forth), the system administrator must configure a primary SMTP email server (and, preferably, a secondary email server).

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **Mail and Notification > Mail Server Configuration**.
  - Step 2** Under Primary SMTP Server, complete the Hostname/IP, User Name, Password, and Confirm Password fields as appropriate for the email server you want Cisco EPN Manager to use. Enter the IP address of the physical server. and the Enter the hostname of the primary SMTP server.
    - Note** You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.
  - Step 3** (Optional) Complete the same fields under Secondary SMTP Server. SMTP server username and password.
  - Step 4** Under Sender and Receivers, enter a legitimate email address for Cisco EPN Manager .
  - Step 5** When you are finished, click **Save**.
-

## Enable FTP/TFTP/SFTP Service on the Server

FTP/TFTP/SFTP is used to transfer files between the server and devices for device configuration and software image file management. These protocols are also used in high availability deployments to transfer files to a secondary server. These services are normally enabled by default. If you installed Cisco EPN Manager in FIPS mode, they are disabled by default. If you use this page to enable these services, Cisco EPN Manager will become non-compliant with FIPS.

SFTP is the secure version of the file transfer service and is used by default. FTP is the unsecured version of the file transfer service; TFTP is the simple, unsecured version of the service. If you want to use either FTP or TFTP, you must enable the service after adding the server.

To change the FTP/TFTP/SFTP password, see [Change the FTP User Password, on page 648](#).

- 
- Step 1** Configure Cisco EPN Manager to use the FTP, TFTP, or SFTP server.
- Choose **Administration > Servers > TFTP/FTP/SFTP Servers**.
  - From the **Select a command** drop-down list, choose **Add TFTP/FTP/SFTP Server**, then click **Go**.
    - From the **Server Type** drop-down list, choose **FTP**, **TFTP**, **SFTP**, or **All**.
    - Enter a user-defined name for the server.
    - Enter the IP address of the server.
  - Click **Save**.
- Step 2** If you want to use FTP or TFTP, enable it on the Cisco EPN Manager server.
- Choose **Administration > Settings > System Settings**, then choose **General > Server**.
  - Go to the FTP or TFTP area.
  - Click **Enable**.
  - Click **Save**.
- Step 3** Restart Cisco EPN Manager to apply your changes. See [Stop and Restart Cisco EPN Manager, on page 647](#).
- 

## Configure Stored Cisco.com Credentials

Cisco EPN Manager can use stored Cisco.com credentials (user name and password) to log in to Cisco.com when it performs the following tasks:

- Checks for product software updates
- Checks for device software image updates
- Opens or reviews Cisco support cases

If these settings are not configured, Cisco EPN Manager will prompt users for their credentials when they perform these tasks. To configure a global Cisco.com user name and password:

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Account Credentials**.

**Step 2** Under the **Cisco.com Credentials** tab, enter a user name and password, and click **Save**.

---

## Create a Login Banner (Login Disclaimer)

When you have a message that you want to display to all users before they log in, create a login disclaimer. The text will be displayed on the GUI client login page below the login and password fields.

---

**Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Login Disclaimer**.

**Step 2** Enter (or edit) the login disclaimer text.

**Note** Carriage returns are ignored.

Your changes will take effect immediately.

---

## Stop and Restart Cisco EPN Manager

An Cisco EPN Manager restart is needed in rare cases, such as after a product software upgrade. When you stop the Cisco EPN Manager server, all user sessions are terminated.

To stop the server, open a CLI session with the server and enter:

```
ncs stop
```

To restart the server, open a CLI session with the server and enter:

```
ncs start
```

## Configure Global SNMP Settings for Communication with Network Elements

The SNMP Settings page controls the how the server uses SNMP to reach and monitor devices. These settings will determine when a device is considered unreachable. Any changes you make on this page are applied globally and are saved across restarts, as well as across backups and restores.



**Note** The default network address is 0.0.0.0, which indicates the entire network. An SNMP credential is defined per network, so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. You should update the prepopulated SNMP credential with your own SNMP information.

---

**Step 1** Choose **Administration > Settings > System Settings**, then choose **Network and Device > SNMP**.

---

- Step 2** (Optional) Select the **Trace Display Values** check box to display mediation trace-level logging data values that are fetched using SNMP.
- Step 3** Choose an algorithm from the **Backoff Algorithm** drop-down list.
- **Exponential**—Each SNMP try will wait twice as long as the previous try, starting with the specified timeout for the first try.
  - **Constant**—Each SNMP try will wait the same length of time (timeout). This is useful on unreliable networks where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.
- Step 4** If you do not want to use the timeout and retries specified by the device, configure the following parameters.
- Note** If switch port tracing is taking a long time to complete, reduce the Reachability Retries value.
- **Reachability Retries**—Enter the number of global retries.
  - **Reachability Timeout**—Enter a global timeout.
- Step 5** In the **MaximumVarBinds per PDU** field, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. This Maximum VarBinds per PDU field enables you to make necessary changes when you have any failures associated to SNMP. For customers who have issues with PDU fragmentation in their network, this number can be reduced to 50, which typically eliminates the fragmentation.
- Step 6** Optionally adjust the **Maximum Rows per Table**.
- Step 7** Click **Save**.
- 

## Manage Administrative Passwords

### Change the FTP User Password

Cisco EPN Manager uses the **ftpuser** ID to access other servers using FTP. Users with Admin privileges can change the FTP password.

- Step 1** Log in to the Cisco EPN Manager server as the admin user. [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).
- Step 2** To change the Cisco EPN Manager server's FTP password, enter:
- ```
ncs password ftpuser username password password
```
- 

#### Example

```
(admin) ncs password ftpuser FTPUser password FTPUserPassword
Initializing...
Updating FTP password.
This may take a few minutes.
Successfully updated location ftpuser
```

## Change the Web GUI Root User Password

Cisco EPN Manager uses the **root** ID to perform special tasks that require root access to the web GUI.

### Before you begin

You must know the current web GUI root user password to change it.

---

**Step 1** Log in to the Cisco EPN Manager Admin CLI as the **root** user. (For information on the Admin CLI, see [User Interfaces and User Types, on page 667](#).)

**Step 2** Enter the following command, where *newpassword* is the new web GUI root password:

```
ncs password root password newpassword
```

---

### Example

```
ncs password root password NewWebGUIRootPassword
Password updated for web root password
```

## Recovering Administrator Passwords on Virtual Appliances

This topic explains how to recover and reset the admin password on Cisco EPN Manager virtual machines (also known as OVAs).

### Before You Begin

Ensure that you have:

- Physical access to the Cisco EPN Manager server.
- A copy of the installation ISO image appropriate for your version of the software.
- Access to the VMware vSphere client, and to the vSphere inventory, Datastores and Objects functions. If you do not have such access, consult your VMware administrator. Avoid accessing ESX directly from the vSphere client.

---

**Step 1** At the Cisco EPN Manager OVA server, launch the VMware vSphere client.

**Step 2** Upload the installation ISO image to the data store on the OVA virtual machine, as follows:

- a) In the vSphere inventory, click **Datastores**.
- b) On the **Objects** tab, select the datastore to which you will upload the file.
- c) Click the **Navigate to the datastore file browser** icon.
- d) If needed, click the **Create a new folder** icon and create a new folder.
- e) Select the folder that you created or select an existing folder, and click the **Upload a File** icon.

If the Client Integration Access Control dialog box appears, click **Allow** to allow the plug-in to access your operating system and proceed with the file upload.

- f) On the local computer, find the ISO file and upload it.
- g) Refresh the datastore file browser to see the uploaded file in the list.

- Step 3** With the ISO image uploaded to a datastore, make it the default boot image, as follows:
- Using the VMware vSphere client, right-click the deployed OVA and choose **Power > Shut down guest**.
  - Select **Edit Settings > Hardware**, then select **CD/DVD drive 1**.
  - Under **Device Type**, select **Datastore ISO File**, then use the **Browse** button to select the ISO image file you uploaded to the datastore.
  - Under **Device Status**, select **Connect at power on**.
  - Click the **Options** tab and select **Boot Options**. Under **Force BIOS Setup**, select **Next time VM boots, force entry into BIOS setup Screen**. This will force a boot from the virtual machine BIOS when you restart the virtual machine.
  - Click **OK**.
  - In the VMware vSphere client, right-click the deployed OVA and choose **Power > Power On**.
  - In the BIOS setup menu, find the option that controls the boot order of devices and move **DVD/CDROM** to the top.
- Step 4** Follow the steps below to reset a server administrator password:
- Save your BIOS settings and exit the BIOS setup menu. The virtual machine will boot from the ISO image and display a list of boot options.
  - Enter **3** if you are using the keyboard and monitor to access the OVA, or **4** if you are accessing via command line or console. The vSphere client displays a list of administrator user names.
  - Enter the number shown next to the administrator username for which you want to reset the password.
  - Enter the new password and verify it with a second entry.
  - Enter **Y** to save your changes and reboot.
  - Once the virtual machine has rebooted: Using the vSphere client, click on the CD icon and select **Disconnect ISO image**.
- Step 5** Log in with the new admin password.

## Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard

The System Monitoring Dashboard provides information about the configuration and performance of the Cisco EPN Manager server. To access the dashboard, choose **Administration > Dashboards > System Monitoring Dashboard** (your User ID must have administrator privileges to access this dashboard). If you want to customize the dashlets that are displayed in the Overview or Performance tabs, follow the instructions in [Add a Predefined Dashlet To a Dashboard, on page 21](#).

Dashboard Tab	Description
<b>Overview</b>	<p>Backup and data purging jobs, Cisco EPN Manager system alarms, and utilization statistics for server CPU, disk, and memory. You can specify different time frames to check this information.</p> <p>To view the server time, kernel version, operating system, hardware information, and so forth, click <b>System Information</b> at the top left of the dashboard to open a field with that information.</p> <p>You can add and delete dashlets from the Overview dashboard.</p>
<b>Performance</b>	<p>Server syslogs and traps, and input/output. You can specify different time frames for this data, and add and remove dashlets from the Performance dashboard.</p>



<b>Admin</b>	<ul style="list-style-type: none"> <li>• Health—System alarms, number of jobs running, number of users logged in, and database usage distribution. You can specify different time frames for historical information.</li> <li>• API Health—Lists all API services with their response time statistics.</li> <li>• Service Details—Statistics for a specific service (response count and time trend, calls per client (clients are identified by their IP address). You can pick the service you want to check.</li> </ul>
--------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Improve the Cisco EPN Manager Server Performance

- [Check the OVA Size, on page 651](#)
- [Compact the Database, on page 651](#)
- [Manage Server Disk Space Issues, on page 651](#)

### Check the OVA Size

If Cisco EPN Manager is using 80 percent or more of your system resources or the device/interface/flow counts recommended for the size of OVA you have installed, this can negatively impact performance. Make sure the OVA is not exceeding the device, interface, and flow record recommendations given in the installation documentation. They are the maximums for each given OVA size. You can check these from the Admin Dashboard (see [Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard, on page 650](#)). To respond to space issues, see [Manage Server Disk Space Issues, on page 651](#).

### Compact the Database

- 
- Step 1** Log in to the server as the admin user. [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#).
- Step 2** Enter the following command to compact the application database:
- ```
(admin) # ncs cleanup
```
- Step 3** When prompted, answer **Yes** to the deep cleanup option.
- 

### Manage Server Disk Space Issues

Cisco EPN Manager will trigger alarms indicating that the server is low on disk space at the following thresholds:

- 60% usage triggers a Major alarm
- 65% usage triggers a Critical alarm

If you receive an alert, consider performing the following actions:

- Free up existing database space as explained in [Compact the Database, on page 651](#).

- If you are saving backups to a local repository, consider using a remote backup repository. See [Set Up NFS-Based Remote Repositories, on page 620](#).
- Reduce the retention period for network inventory, performance, reports, and other classes of data as explained in [Data Collection and Purging, on page 655](#).
- Add more disk space. VMware OVA technology enables you to easily add disk space to an existing server. You will need to shut down the Cisco EPN Manager server and then follow the [instructions provided by VMware](#) to expand the physical disk space. Once you restart the virtual appliance, Cisco EPN Manager automatically makes use of the additional disk space (see [Data Collection and Purging, on page 655](#)).
- Set up a new server that meets at least the minimum RAM, disk space, and processor requirements of the next higher level of OVA. Back up your existing system, then restore it to a virtual machine on the higher-rated server.

## Work With Server Internal SNMP Traps That Indicate System Problems

Cisco EPN Manager generates internal SNMP traps that indicate potential problems with system components. This includes hardware component failures, high availability state changes, backup status, and so forth. The failure trap is generated as soon as the failure or state change is detected, and a clearing trap is generated if the failure corrects itself. For TCAs (high CPU, memory and disk utilization traps, and so forth), the trap is generated when the threshold is exceeded.

A complete list of server internal SNMP traps is provided in [Cisco Evolved Programmable Network Manager Supported Alarms](#). Cisco EPN Manager sends traps to notification destination on port 162. This port cannot be customized at present.

You can customize and manage these traps as described in the following topics:

- [Customize Server Internal SNMP Traps and Forward the Traps, on page 652](#)
- [Troubleshoot Server Internal SNMP Traps, on page 653](#)

## Customize Server Internal SNMP Traps and Forward the Traps

You can customize server internal SNMP traps by adjusting their severity or (for TCAs) thresholds. You can also disable and enable the traps. Server internal SNMP traps are listed in [Cisco Evolved Programmable Network Manager Supported Alarms](#).




---

**Note** Cisco EPN Manager does not send SNMPv2 Inform or SNMPv3 notifications.

---

**Step 1** Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > System Event Configuration**.

**Step 2** For each SNMP event you want to configure:

- Click on the row for that event.
- Set the **Event Severity** to Critical, Major, or Minor, as needed.

- c) For the CPU, disk, memory utilization, and other hardware traps, Enter the **Threshold** percentage (from 1–99). These events will send the associated SNMP traps when the utilization exceeds the threshold limit. (You cannot set thresholds for events for which the threshold setting is shown as NE.) These events send traps whenever the associated failure is detected.
- d) For backup threshold and certificate expiry (critical), enter the **Threshold** in days (from  $x$ – $y$ , where  $x$  is the minimum number of days and  $y$  is the maximum number of days).
- e) To control whether a trap is or is not generated, set the **Event Status**.

**Step 3** To save all of your trap changes, click **Save** (below the table).

**Step 4** If you want to configure receivers for the server internal SNMP traps, refer to the procedures in the following topics, depending on whether you want to send the information as an email or trap notification.

- [Forward Alarms and Events as Email Notifications \(Administrator Procedure\), on page 706](#)
- [Forward Alarms and Events as SNMP Trap Notifications, on page 707](#)

---

## Troubleshoot Server Internal SNMP Traps

[Cisco Evolved Programmable Network Manager Supported Alarms](#) provides a complete list of server internal SNMP traps, their probable cause, and recommended actions to remedy the problem. If that document does not provide the information you need, follow this procedure to troubleshoot and get more information about Cisco EPN Manager server issues.

---

**Step 1** Ping the notification receiver from the Cisco EPN Manager server to ensure that there is connectivity between Cisco EPN Manager and your management application.

**Step 2** Check if any firewall ACL settings are blocking port 162, and open communications on that port if needed.

**Step 3** Log in to Cisco EPN Manager with a user ID that has Administrator privileges. Select **Administration > Logging** and download the log files. Then compare the activity recorded in these log files with the activity you are seeing in your management application:

- ncs\_nbi.log: This is the log of all the northbound SNMP trap messages Cisco EPN Manager has sent. Check for messages you have not received.
- ncs-#-#.log: This is the log of most other recent Cisco EPN Manager activity. Check for hardware trap messages you have not received.
- hm-#-#.log: This is the log of all Health Monitor activity. Check for recent messages about High Availability state-changes and application-process failures that you have not received.

The messages you see in these logs should match the activity you see in your management application. If you find major differences, open a support case with Cisco Technical Assistance Center (TAC) and attach the suspect log files with your case. See [Open a Cisco Support Case, on page 714](#).

---

## Set Up Defaults for Cisco Support Requests

By default, users can create Cisco support requests from different parts of the Cisco EPN Manager GUI. If desired, you can configure the sender e-mail address and other e-mail characteristics. If you do not configure them, users can supply the information when they open a case.

If you do not want to allow users to create requests from the GUI client, you can disable that feature.

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Account Settings**.
- Step 2** Click the **Support Request** tab.
- Step 3** Select the type of interaction you prefer:
- Enable interactions directly from the server—Specify this option to create the support case directly from the Cisco EPN Manager server. E-Mails to the support provider are sent from the e-mail address associated with the Cisco EPN Manager server or the e-mail address you specify.
  - Interactions via client system only—Specify this option to download the information required for your support case to a client machine. You must then e-mail the downloaded support case details and information to the support provider.
- Step 4** Select your technical support provider:
- Click **Cisco** to open a support case with Cisco Technical Support, enter your Cisco.com credentials, then click **Test Connectivity** to check the connectivity to the following servers:
    - Cisco EPN Manager mail server
    - Cisco support server
    - Forum server
  - Click **Third-party Support Provider** to create a service request with a third-party support provider. Enter the provider's e-mail address, the subject line, and the website URL.
- 

## Configure Cisco Product Feedback Settings

To help Cisco improve its products, Cisco EPN Manager collects the following data and sends it to Cisco:

- Product information—Product type, software version, and installed licenses.
- System information—Server operating system and available memory.
- Network information—Number and type of devices on your network.

This feature is enabled by default. Data is collected on a daily, weekly, and monthly basis and is posted to a REST URL in the Cisco cloud using HTTPS. Choose **Administration > Settings > System Settings**, then choose **General > Help Us Improve**, and:

- To view the types of data Cisco collects, click **What data is Cisco collecting?**
- To disable this feature, select **Not at this time, thank you**, then click **Save**.



## CHAPTER 24

# Data Collection and Purging

- [Control Data Collection Jobs](#), on page 655
- [How Data Retention Settings Affect Web GUI Data](#), on page 663
- [Performance and System Health Data Retention](#), on page 663
- [Alarm, Event, and Syslog Purging](#), on page 664
- [Log Purging](#), on page 665
- [Report Purging](#), on page 665
- [Backup Purging](#), on page 665
- [Device Configuration File Purging](#), on page 666
- [Software Image File Purging](#), on page 666

## Control Data Collection Jobs

All data collection tasks (and data purging tasks) are controlled from the Jobs Dashboard. See [Manage Jobs Using the Jobs Dashboard](#), on page 25. Data collection jobs are listed under System Jobs .

## About System Jobs

The following table describes the background data collection jobs Cisco EPN Manager performs.

**Table 46: Inventory Data Collection Jobs**

| Task Name                       | Default Schedule | Description                                                                            | Editable options                                                                                     |
|---------------------------------|------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>APIC EM Integration Jobs</b> | 6 hours          | Schedules synchronization of sites and devices between APIC-EM and Cisco EPN Manager . | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| APIC-EM Site Sync               |                  |                                                                                        |                                                                                                      |
| APIC Server Status Periodic     | 5 minutes        | Schedules checks on APIC-EM server reachability.                                       | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |

| Task Name                       | Default Schedule | Description                                                                                                                                                                                                             | Editable options                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PnP Status Polling              | 5 minutes        | Tracks the status of the PnP devices created on APIC-EM and adds them to Prime Inventory when successful.                                                                                                               | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job.                                                                                                                                                                                                                                                                |
| <b>Infrastructure jobs</b>      |                  |                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                         |
| Mobility Service Status         | 5 minutes        | Schedules mobility services status polling.                                                                                                                                                                             | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job.                                                                                                                                                                                                                                                                |
| Autonomous Client Status        | 5 minutes        | Lets you schedule status polling of autonomous AP clients.                                                                                                                                                              | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job.                                                                                                                                                                                                                                                                |
| Bulk Recompute RF Prediction    | 15 days          | Schedules status polling of Bulk Recompute RF Prediction.                                                                                                                                                               | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job.                                                                                                                                                                                                                                                                |
| Controller Configuration Backup | 1 day            | Displays the controller configuration backup activities.                                                                                                                                                                | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job.                                                                                                                                                                                                                                                                |
| Data Cleanup                    | 2 hours          | Schedules daily data file cleanup.                                                                                                                                                                                      | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job.                                                                                                                                                                                                                                                                |
| Device Config Backup-External   | 15 minutes       | Transfers device configuration periodically to external repository. You can configure or create the repository using CLI commands and the supported repositories are FTP, SSH FTP (SFTP) and Network File System (NFS). | <p>Select <b>Edit Schedule</b> &gt; <b>Recurrence</b> and select the appropriate settings to schedule the job.</p> <p>Click the edit icon, and check the <b>Export only Latest Configuration</b> check box, to transfer only the latest configuration.</p> <p>You can edit the job properties based on the user permission set in Role Based Access Control (RBAC).</p> |
| Guest Accounts Sync             | 1 day            | Schedules guest account polling and synchronization.                                                                                                                                                                    | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job.                                                                                                                                                                                                                                                                |

| Task Name                           | Default Schedule | Description                                                                                        | Editable options                                                                                     |
|-------------------------------------|------------------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Index Search Entities               | 3 hours          | Schedules the Index Search Entities job.                                                           | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Mobility Service Backup             | 7 days           | Schedules automatic mobility services backups.                                                     | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Mobility Service Synchronization    | 1 hour           | Schedules mobility services synchronization.                                                       | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| On Demand Reports Cleanup           | 6 hours          | Schedules reports cleanup.                                                                         | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Server Backup                       | 1 day            | Schedules automatic Cisco EPN Manager server backups. The backups created are application backups. | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Smart License Compliance Status     | Disabled         | Runs for Smart License for the default schedule.                                                   | Non Editable.                                                                                        |
| wIPS Alarm Sync                     | 2 hours          | Schedules wIPS alarm synchronization.                                                              | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| <b>Inventory and Discovery Jobs</b> |                  |                                                                                                    |                                                                                                      |
| Autonomous AP Inventory             | 1 day            | Collects inventory information for autonomous APs.                                                 | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Switch Inventory                    | 1 day            | Collects inventory information for Switches.                                                       | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Wireless Controller Inventory       | 1 day            | Collects inventory information for Wireless Controllers.                                           | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| <b>Status Jobs</b>                  |                  |                                                                                                    |                                                                                                      |

| Task Name                                | Default Schedule | Description                                                                                                                                                                                                                                      | Editable options                                                                                         |
|------------------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Appliance Status                         | 5 minutes        | Schedules appliance polling. This task populates the appliance polling details from the Administration > Appliance > Appliance Status page. It also populates information like the performance and fault checking capabilities of the appliance. | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| Autonomous AP Operational Status         | 5 minutes        | Schedules status polling of autonomous wireless access points.                                                                                                                                                                                   | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| Controller Operational Status            | 5 minutes        | Schedules controller operational status polling.                                                                                                                                                                                                 | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| Device Data Collector                    | 30 minutes       | Schedules data collection based on specified command-line interface (CLI) commands at a configured time interval.                                                                                                                                | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| Identity Services Engine Status          | 15 minutes       | Schedules Identity Services Engine polling.                                                                                                                                                                                                      | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| Interferers                              | 15 minutes       | Schedules interferer information collection.                                                                                                                                                                                                     | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| License Status                           | 4 hours          | Schedules the license-status information collection.                                                                                                                                                                                             | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| Lightweight AP Ethernet Interface Status | 1 minute         | Schedules Lightweight AP Ethernet Interface Status information collection.                                                                                                                                                                       | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| Lightweight AP Operational Status        | 5 minutes        | Schedules Lightweight AP Operational Status information collection.                                                                                                                                                                              | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |



| Task Name                                   | Default Schedule | Description                                                                                   | Editable options                                                                                     |
|---------------------------------------------|------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Lightweight Client Status                   | 5 minutes        | Schedules information collection for Lightweight AP Clients from Network.                     | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Mobility Service Performance                | 15 minutes       | Schedules status polling of mobility services performance.                                    | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Mobility Status Task                        | 15 minutes       | Schedules status polling of mobility services engines.                                        | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| OSS Server Status                           | 5 minutes        | Schedules status polling of OSS Servers.                                                      | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Redundancy Status                           | 1 hour           | Schedules redundancy status polling of primary and secondary controllers.                     | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Switch NMSP and Location Status             | 4 hours          | Schedules Switch Network Mobility Services Protocol (NMSP) and Civic Location status polling. | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Switch Operational Status                   | 5 minutes        | Schedules switch operational status polling.                                                  | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Third Party Access Point Operational Status | 3 hours          | Schedules operational status polling of third party APs.                                      | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Third Party Controller Operational Status   | 3 hours          | Schedules operational status polling of third party Controllers.                              | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Unmanaged APs                               | 15 minutes       | Collects poll information for unmanaged access points.                                        | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |

| Task Name                          | Default Schedule | Description                                              | Editable options                                                                                     |
|------------------------------------|------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Wired Client Status                | 2 hours          | Schedules Wireless Client status polling                 | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Wireless AP Discovery              | 5 minutes        | Schedules Wireless AP discovery.                         | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Wireless Configuration Audit       | 1 day            | Schedules Wireless Configuration Agent audit collection. | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| <b>Utilization Collection Jobs</b> |                  |                                                          |                                                                                                      |
| UtilizationCollector_15Min         | 15 minutes       | Schedules physical interface utilization.                | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| UtilizationProvider_15Min          | 15 minutes       | Schedules physical links utilization.                    | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| UtilizationCollector_1Hour         | 1 hour           | Schedules physical interface utilization.                | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| UtilizationProvider_1h             | 1 hour           | Schedules physical links utilization.                    | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| UtilizationCollector_6Hour         | 6 hours          | Schedules physical interface utilization.                | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| UtilizationProvider_6h             | 6 hours          | Schedules physical links utilization.                    | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| UtilizationCollector_24Hour        | 24 hours         | Schedules physical interface utilization.                | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |

| Task Name                                      | Default Schedule | Description                                                                                                                                                                                                                                   | Editable options                                                                                     |
|------------------------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| UtilizationProvider_1d                         | 24 hours         | Schedules physical links utilization.                                                                                                                                                                                                         | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| <b>Wireless Monitoring Jobs</b>                |                  |                                                                                                                                                                                                                                               |                                                                                                      |
| AP Ethernet Statistics                         | 15 minutes       | Schedules AP Ethernet statistics collection.                                                                                                                                                                                                  | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| AP Image Pre-Download Status                   | 15 minutes       | Allows you to see the Image Predownload status of the associated APs in the controllers. To see the status of the access points, the “Pre-download software to APs” checkbox should be selected while downloading software to the controller. | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Autonomous AP CPU and Memory Utilization       | 15 minutes       | Schedules collection of information on memory and CPU utilization of Autonomous APs.                                                                                                                                                          | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Autonomous AP Radio Performance                | 15 minutes       | Schedules collection of information about radio performance information as well as radio up or down status for autonomous APs.                                                                                                                | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Autonomous AP Tx Power and Channel Utilization | 15 minutes       | Schedules collection of information about radio performance of Autonomous APs.                                                                                                                                                                | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| CCX Client Statistics                          | 1 hour           | Schedules collection of the Dot11 and security statistics for CCX Version 5 and Version 6 clients.                                                                                                                                            | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| CleanAir Air Quality                           | 15 minutes       | Schedules collection of information about CleanAir air quality.                                                                                                                                                                               | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |

| Task Name                  | Default Schedule | Description                                                                            | Editable options                                                                                     |
|----------------------------|------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Client Statistics          | 15 minutes       | Schedules retrieval of statistical information for autonomous and lightweight clients. | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Map Info Polling Job       | 1 minute         |                                                                                        | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Media Stream Clients       | 15 minutes       | Schedules collection of information about media stream clients.                        | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Mesh Link Status           | 5 minutes        | Schedules collection of status of mesh links.                                          | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Mesh link Performance      | 10 minutes       | Schedules collection of information about the performance of mesh links.               | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Radio Performance          | 15 minutes       | Schedules collection of statistics from wireless radios.                               | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Radio Voice Performance    | 15 minutes       | Schedules collection of voice statistics from wireless radios.                         | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Rogue AP                   | 2 hours          | Schedules collection of information about rogue access points.                         | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Switch CPU and Memory Poll | 30 minutes       | Schedules polling of switch CPU and memory information.                                | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |
| Traffic Stream Metrics     | 8 minutes        | Retrieves traffic stream metrics for the clients.                                      | Select <b>Edit Schedule &gt; Recurrence</b> and select the appropriate settings to schedule the job. |

| Task Name                       | Default Schedule | Description                                                                  | Editable options                                                                                         |
|---------------------------------|------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Wireless Controller Performance | 30 minutes       | Schedules collection of performance statistics for wireless controllers.     | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |
| Wireless QoS Statistics         | 15 minutes       | Schedules collection of information QoS Statistics for Wireless Controllers. | Select <b>Edit Schedule</b> > <b>Recurrence</b> and select the appropriate settings to schedule the job. |

## How Data Retention Settings Affect Web GUI Data

Changes you make on the Data Retention page determine the information that is displayed in the web GUI. You can open the data retention page by choosing **Administration** > **Settings** > **System Settings**, then choosing **General** > **Data Retention**.

For example, if you do not need any historical performance data older than 7 days, you can modify the performance data retention values as follows:

- Short-term Data Retention Period—1 day
- Medium-term Data Retention Period—3 days
- Long-term Data Retention Period—7 days

If you specify these settings, all data displayed in performance reports and on performance dashboards will be for the previous 7 days only. When you generate a performance report, even if you select a reporting period longer than the last 7 days, the report will contain data from the last 7 days only (because that is all of the data you selected to retain).

Similarly, if you view a performance dashboard and select a time frame longer than one week, the dashboard will contain data from the last 7 days only.

## Performance and System Health Data Retention



**Note** Cisco recommends you do not change the retention periods for trend, device health, system health, and performance data because the default settings are optimized to get the most helpful information from interactive graphs.

The following table describes the information shown on the Data Retention page.

| Type of Data  | Description                                                                                                                                                                                                                            | Default Retention Settings                                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Trend         | Device-related historical information. Trend data is gathered as a whole and summarized as minimums, maximums, or averages.                                                                                                            | Hourly data: 15<br>Daily data: 90<br>Weekly data: 54 weeks             |
| Device health | SNMP-polled device data such as device reachability, and utilization for CPU, memory, and interfaces.                                                                                                                                  | Hourly data: 15<br>Daily data: 90<br>Weekly data: 54 weeks             |
| Performance   | Assurance data such as traffic statistics. <ul style="list-style-type: none"> <li>Short-term data is aggregated every 5 minutes.</li> <li>Medium-term data is aggregated every hour.</li> <li>Long-term is aggregated daily</li> </ul> | Short-term data: 7<br>Medium-term data: 31<br>Long-term data: 365 days |
| Network audit | Audit records for configurations triggered by users, and so on.                                                                                                                                                                        | 90 days                                                                |
| System health | Includes most data shown on the Admin dashboards                                                                                                                                                                                       | Hourly data: 15<br>Daily data: 90<br>Weekly data: 54 weeks             |

For example, these are the retention settings for optical performance data:

- Optical 15-minute performance data (short-term) is saved for 7 days.
- Optical 1-day performance data (medium-term) is saved for 31 days.

## Alarm, Event, and Syslog Purging



### Note

These default purging settings are provided to ensure optimal performance. Use care when adjusting these settings, especially if Cisco EPN Manager is managing a very large network (where increasing these settings may have an adverse impact).

Cisco EPN Manager stores a maximum of 8000000 events and 2000000 syslogs in the database.

To protect system performance, Cisco EPN Manager purges alarms, events, and syslogs according to the settings in the following table. All of these settings are enabled by default. Data is deleted on a daily basis. Alarm tables are checked hourly, and if the alarm table exceeds the 300,000 limit, Cisco EPN Manager deletes the oldest cleared alarms until the alarms table size is within the limit.

| Data Type                          | Deleted after: | Default Setting |
|------------------------------------|----------------|-----------------|
| Alarms—Cleared security alarms     | 30 days        | Enabled         |
| Alarms—Cleared non-security alarms | 7 days         | Enabled         |

|         |         |          |
|---------|---------|----------|
| Events  | 60 days | Enabled  |
| Syslogs | 30 days | Enabled  |
| Alarms  | 30 days | Disabled |

To change the settings, choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarms and Events** and modify the settings in the Alarm and Event Cleanup Options area.

## Log Purging

You can adjust the purging settings for logs by choosing **Administration > Settings > Logging**. Logs are saved until they reach the maximum size. At that point, a number is appended to the log file and a new log is started. When the number of logs exceeds the maximum, the oldest log is deleted.

The following table lists the default purging values for General and SNMP logs.

| Log Type | Size of Logs | Number of Logs | To change the setting, see:                                                     |
|----------|--------------|----------------|---------------------------------------------------------------------------------|
| General  | 10 MB        | 10             | <a href="#">Adjust General Log File Settings and Default Sizes, on page 720</a> |
| SNMP     | 10 MB        | 5              | <a href="#">View and Manage General System Logs, on page 720</a>                |

## Report Purging

By default, reports are stored in a repository named `/localdisk/ftp/reports` and are deleted after 31 days from that directory. Reports filters that you set from the filters page are saved in the database and are not purged.

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Reports**.
  - Step 2** If required, adjust the location for the reports repository on the server. The repository must reside under the FTP root partition.
  - Step 3** If you want to change the default purging age, enter a new value in the **File Retain Period** field.
  - Step 4** Click **Save**.
- 

## Backup Purging

By default, 2 backups are saved for backups in local repositories. If you are using remote repositories, there is no automatic backup purging mechanism; you must manually delete old backups. See [Change the Number of Automatic Application Backups That Are Saved, on page 625](#).

## Device Configuration File Purging

For each device, 5 configuration files are saved in the configuration archive. Any file that is older than 30 days is purged. Device configuration files cannot be manually deleted. For more information on device configuration files, see [Manage Device Configuration Files, on page 91](#).

## Software Image File Purging

Device software image files are not automatically purged from the database. They must be manually removed using the GUI client. For more information, see [Delete Software Image Files from the Image Repository, on page 132](#).





## CHAPTER 25

# User Permissions and Device Access

---

- [User Interfaces, User Types, and How To Transition Between Them, on page 667](#)
- [Enable and Disable root Access for the Linux CLI and the Cisco EPN Manager Web GUI, on page 671](#)
- [Control the Tasks Users Can Perform \(User Groups\), on page 672](#)
- [Add Users and Manage User Accounts, on page 677](#)
- [Find Out Which Users Are Currently Logged In, on page 679](#)
- [View the Tasks Performed By Users \(Audit Trail\), on page 680](#)
- [Configure Job Approvers and Approve Jobs, on page 680](#)
- [Configure Global Password Policies for Local Authentication, on page 681](#)
- [Configure the Global Timeout for Idle Users, on page 681](#)
- [Create Virtual Domains to Control User Access to Devices, on page 682](#)
- [Configure Local Authentication, on page 690](#)
- [Configure External Authentication, on page 691](#)

## User Interfaces, User Types, and How To Transition Between Them

These topics describe the GUI and CLI interfaces used by Cisco EPN Manager , and how to transition between the Cisco EPN Manager and Linux CLI interfaces.

- [User Interfaces and User Types, on page 667](#)
- [How to Transition Between the CLI User Interfaces in Cisco EPN Manager , on page 669](#)

## User Interfaces and User Types

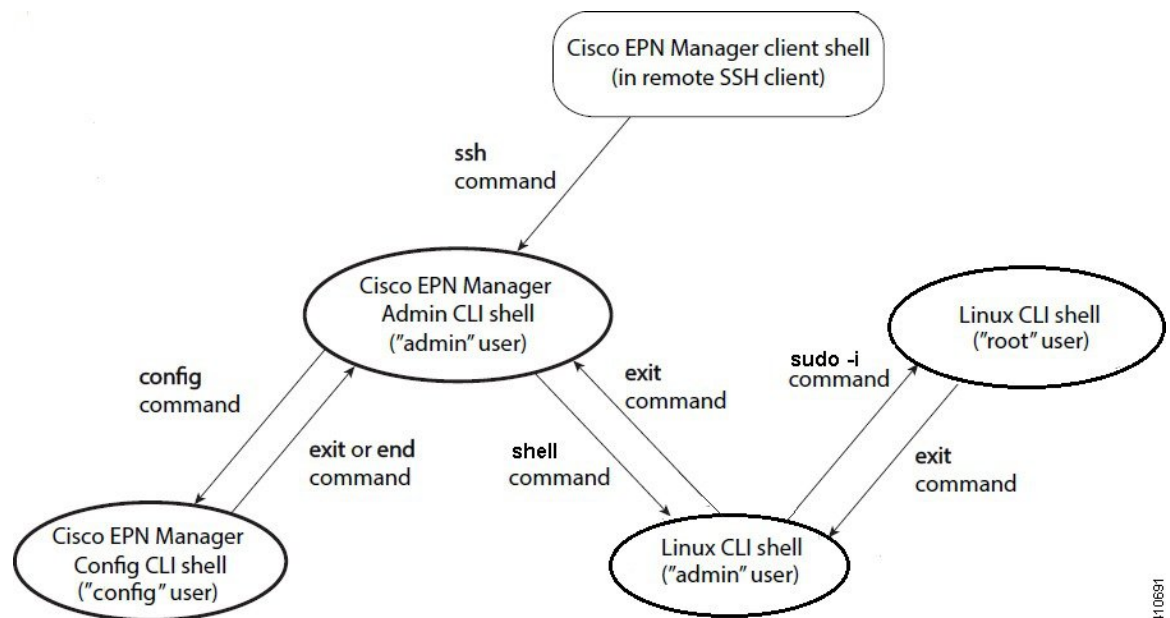
The following table describes the user interfaces employed by Cisco EPN Manager (CEPNM), and the types of users that can access each interface.

| CEPNM User Interface | Interface Description                                                                                                                                                                                                                                                                                                                                                                                        | CEPNM User Types                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CEPNM web GUI        | <p>Web interface that facilitates day-to-day and administration operations using the web GUI. These users can have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses.</p> <p>This interface provides a subset of operations that are provided by the Cisco EPN Manager CLI admin and CLI config users.</p>                                       | <p><b>Cisco EPN Manager web GUI everyday users</b>—Created by web GUI root user . These users have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses called <i>user groups</i> (Admin, Super Users, Config Managers, and so forth). For information on the user groups, see <a href="#">Types of User Groups, on page 672</a>.</p> <p><b>Cisco EPN Manager web GUI root user</b>—Created at installation and intended for first-time login to the web GUI, and for creating other user accounts. This account should be disabled after creating at least one web GUI user that has Admin privileges—that is, a web GUI user that belongs to the Admin or Super Users user group. See <a href="#">Disable and Enable the Web GUI root User, on page 671</a>.</p> <p><b>Note</b> The Cisco EPN Manager web GUI root user is not the same as the Linux CLI root user, nor is it the same as the Cisco EPN Manager CLI admin user.</p> |
| CEPNM Admin CLI      | Cisco proprietary shell which provides secure and restricted access to the system (as compared with the Linux shell). This Admin shell and CLI provide commands for advanced Cisco EPN Manager administration tasks. These commands are explained throughout this guide. To use this CLI, you must have Cisco EPN Manager CLI admin user access. You can access this shell from a remote computer using SSH. | <p><b>Cisco EPN Manager CLI Admin user</b>—Created at installation time and used for administration operations such as stopping and restarting the application and creating remote backup repositories. (A subset of these administration operations are available from the web GUI).</p> <p>To display a list of operations this user can perform, enter ? at the prompt.</p> <p>Some tasks must be performed in config mode. To transition to config mode, use the procedure in <a href="#">Transition Between the Cisco EPN Manager admin CLI and Cisco EPN Manager config CLI, on page 669</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                        |
| CEPNM Config CLI     | Cisco proprietary shell which is restricted and more secure than the Linux shell. This Config shell and CLI provide commands for Cisco EPN Manager system configuration tasks. These commands are explained throughout this guide. To use this CLI, you must have admin-level user access (see the information in the User Types column of this table). You can access this shell from the Admin CLI shell.  | <p>The admin CLI user can create other CLI users for a variety of reasons, using the following command:</p> <pre>(config) username username password role {admin user} password</pre> <p>These users may have admin-like privilege/roles or lower level privileges as defined during creation time. To create a Cisco EPN Manager CLI user with admin privileges, run the <b>username</b> command with the <b>admin</b> keyword; otherwise, use the <b>user</b> keyword.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| CEPNM User Interface | Interface Description                                                                                                                                                                                                                                                                                                               | CEPNM User Types                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Linux CLI            | Linux shell which provides all Linux commands. The Linux shell should only be used by Cisco technical support representatives. Regular system administrators should not use the Linux shell. You cannot reach this shell from a remote computer using SSH; you can only reach it through the Cisco EPN Manager admin shell and CLI. | <p><b>Linux CLI admin user</b>—Created at installation time and used for Linux-level administration purposes.</p> <p>This admin user can get root-level privileges by following the procedure in <a href="#">Log In and Out as the Linux CLI root User, on page 670</a>. Tasks that require root-level permissions should only be performed by Cisco Support teams to debug product-related operational issues. For security purposes, the Linux CLI admin and root users should be disabled; see <a href="#">Disable and Enable the Linux CLI Users in Cisco EPN Manager 2.x, on page 671</a>.</p> |

## How to Transition Between the CLI User Interfaces in Cisco EPN Manager

The following figure illustrates how to transition between the Cisco EPN Manager and Linux CLI user interfaces on deployments running Cisco EPN Manager .



410631

### Transition Between the Cisco EPN Manager admin CLI and Cisco EPN Manager config CLI

To move from the Cisco EPN Manager admin CLI to the Cisco EPN Manager config CLI, enter **config** at the admin prompt.

```
(admin) # config
(config) #
```

To move from the config CLI back to the admin CLI, enter **exit** or **end** at the config prompt:

```
(config) # exit
(admin) #
```

## Log In and Out as the Linux CLI root User

The Linux CLI has two shell users: One with administrative access (Linux CLI admin user), and another with root access (Linux CLI root user). The diagram in [How to Transition Between the CLI User Interfaces in Cisco EPN Manager , on page 669](#) illustrates the flow for logging in and out as the various CLI users.

To log in as the Linux CLI root user, you will have to transition from being the Cisco EPN Manager CLI admin user to the Linux CLI admin user to the Linux CLI root user. The following procedure gives you the exact steps you must follow.

### Before you begin

If the Linux CLI user is disabled, re-enable it. See [Disable and Enable the Linux CLI Users in Cisco EPN Manager 2.x, on page 671](#).

---

#### Step 1 To log in as the Linux CLI root user:

- a) Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
- b) As the Cisco EPN Manager CLI admin user, log in as the Linux CLI admin user:

```
shell
Enter shell access password: password
```

- c) Log in as the Linux CLI root user.

```
sudo -i
```

By default, the Linux CLI shell prompt is the same for the Linux CLI admin and root user. You can use the **whoami** command to check the current user.

#### Step 2 To exit:

- a) Log out as the Linux CLI root user.

```
exit
```

- b) Log out as the Linux CLI admin user.

```
exit
```

You are now logged in as the Cisco EPN Manager CLI admin user.

---

### What to do next

For security purposes, disable the Linux CLI root user. See [Disable and Enable the Linux CLI Users in Cisco EPN Manager 2.x, on page 671](#).

# Enable and Disable root Access for the Linux CLI and the Cisco EPN Manager Web GUI

As described in [How to Transition Between the CLI User Interfaces in Cisco EPN Manager](#), on page 669, after installation, you should disable the Cisco EPN Manager web GUI **root** user after creating at least one other web GUI user that has Admin or Super Users privileges. See [Disable and Enable the Web GUI root User](#), on page 671.

The Linux CLI root user is disabled after installation time. If you need to re-enable it, follow the procedure in [Disable and Enable the Linux CLI Users in Cisco EPN Manager 2.x](#), on page 671.

## Disable and Enable the Linux CLI Users in Cisco EPN Manager 2.x

This procedure shows you how to disable and enable the Linux CLI admin shell in deployments running Cisco EPN Manager 2.x. When you disable the shell, you will no longer be able to log in as the Linux CLI admin or root users. When the shell is enabled, users can log in by following the procedure in [How to Transition Between the CLI User Interfaces in Cisco EPN Manager](#), on page 669.

### Before you begin

Make sure you have the password for the Linux CLI admin user.

---

**Step 1** Log in to Cisco EPN Manager as the Cisco EPN Manager CLI admin user. See [Establish an SSH Session With the Cisco EPN Manager Server](#), on page 644.

**Step 2** Disable the Linux CLI admin shell (which disables the Linux CLI admin and root users):

```
shell disable
Enter shell access password: passwd
shell access is disabled
```

**Step 3** To re-enable the Linux CLI admin shell (you must run this command as the Cisco EPN Manager CLI admin user):

```
shell
Shell access password is not set
Configure password for shell access

Password: passwd
Password again: passwd

Shell access password is set
Run the command again to enter shell
```

---

## Disable and Enable the Web GUI root User

---

**Step 1** Log into the Cisco EPN Manager web GUI as root, and create another web GUI user that has root privileges—that is, a web GUI user that belongs to the Admin or Super Users user group. See [Add Users and Manage User Accounts](#), on page 677. Once this is done, you can disable the web GUI **root** account.

**Step 2** Disable the Cisco EPN Manager web GUI root user account. (The web GUI admin account, which remains active, can perform all required CLI functions.)

```
ncs webroot disable
```

**Step 3** To re-enable the account:

```
ncs webroot enable
```

---

## Control the Tasks Users Can Perform (User Groups)

Cisco EPN Manager user authorization is implemented through user groups. A user group contains a list of tasks that control which parts of Cisco EPN Manager a user can access and the tasks the user can perform in those parts.

While user groups control what the user can do, *virtual domains* control the devices on which a user can perform those tasks. Virtual domains are described in [Create Virtual Domains to Control User Access to Devices, on page 682](#).

Cisco EPN Manager provides several predefined user groups. If a user belongs to a user group, the user inherits all of the authorization settings for that group. A user is normally added to user groups when their account is created.

These topics explain how to manage user authorization:

- [Types of User Groups, on page 672](#)
- [View and Change the Tasks a User Can Perform, on page 674](#)
- [View and Change the Groups a User Belongs To, on page 674](#)
- [View User Groups and Their Members, on page 675](#)
- [Create a Customized User Group, on page 675](#)
- [View and Change the Tasks a Group Can Perform, on page 676](#)
- [Use Cisco EPN Manager User Groups with RADIUS and TACACS+, on page 676](#)

## Types of User Groups

Cisco EPN Manager provides the following predefined user groups:

- [User Groups—Web UI, on page 672](#)
- [User Groups—NBI, on page 673](#)

For information about CLI users, see [User Interfaces and User Types, on page 667](#).

### User Groups—Web UI

Cisco EPN Manager provides the default web GUI user groups listed in the following table. You can assign users to multiple groups, except for users that belong to the Monitor Lite user group (because Monitor Lite is meant for users who should have very limited permissions).

See [View and Change the Tasks a Group Can Perform, on page 676](#) for information on the tasks that pertain to each user group and the default settings.

| User Group        | Group Task Focus                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root              | All operations. The group permissions are not editable. The root web UI user is available after installation and is described in <a href="#">User Interfaces and User Types, on page 667</a> . A best practice is to create other users with Admin or Super Users privileges, and then disable the root web UI user as described in <a href="#">Disable and Enable the Web GUI root User, on page 671</a> . |
| Super Users       | All operations (similar to root). The group permissions are editable.                                                                                                                                                                                                                                                                                                                                       |
| Admin             | Administer the system and server. Can also perform monitoring and configuration operations. The group permissions are editable.                                                                                                                                                                                                                                                                             |
| Config Managers   | Configure and monitor the network (no administration tasks). The permissions assigned to this group are editable.                                                                                                                                                                                                                                                                                           |
| System Monitoring | Monitor the network (no configuration tasks). The group permissions are editable.                                                                                                                                                                                                                                                                                                                           |
| Help Desk Admin   | Only has access to the help desk and user preferences related pages. Members of this user group cannot be members of any other user group. This is a special group which lacks access to the user interface.                                                                                                                                                                                                |
| Lobby Ambassador  | User administration for Guest users only. Members of this user group cannot be members of any other user group.                                                                                                                                                                                                                                                                                             |
| User-Defined 1–4  | N/A; these are blank groups and can be edited and customized as needed.                                                                                                                                                                                                                                                                                                                                     |
| Monitor Lite      | View network topology and use tags. The group permissions are not editable. Members of this user group cannot be members of any other user group.                                                                                                                                                                                                                                                           |
| North Bound API   | Access to the SOAP APIs.                                                                                                                                                                                                                                                                                                                                                                                    |
| User Assistant    | Local Net user administration only. Members of this user group cannot be members of any other user group.                                                                                                                                                                                                                                                                                                   |
| mDNS Policy Admin | mDNS policy administration functions.                                                                                                                                                                                                                                                                                                                                                                       |

## User Groups—NBI

Cisco EPN Manager provides the default NBI user groups listed in the following table. The permissions in these groups are not editable.

See [View and Change the Tasks a Group Can Perform, on page 676](#) for information on the tasks that pertain to each user group and the default settings.

| User Group     | Provides access to:                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------|
| NBI Credential | Credential management using MTOSI NBI. Can also belong to other NBI and web UI user groups.             |
| NBI Read       | MTOSI and RESTCONF NBI read operations (HTTP GET). Can also belong to other NBI and web UI user groups. |

| User Group | Provides access to:                                                                                                    |
|------------|------------------------------------------------------------------------------------------------------------------------|
| NBI Write  | MTOSI and RESTCONF NBI write operations (HTTP PUT, POST, DELETE). Can also belong to other NBI and web UI user groups. |

## View and Change the Tasks a User Can Perform

The tasks a user can perform is controlled by the user groups the user belongs to. Follow these steps to find out which groups a user belongs to and which tasks a user is authorized to perform.



**Note** If you want to check the *devices* a user can access, see [Assign Virtual Domains to Users, on page 687](#).

- 
- Step 1** Choose **Administration > Users > Users, Roles & AAA** and locate the user name.
- Step 2** Locate the user name and check the **Member of** column to find out which user groups the user belongs to.
- Step 3** Click a user group hyperlink. The **Group Detail** window lists the tasks that group members can and cannot perform.
- A checked check box means group members have permission to perform that task. If a checked box is greyed-out, it means you cannot disable the task. For example, Cisco EPN Manager does not allow you to remove the "View tags" task for the Monitor Lite user group because it is an integral task for that user group.
  - A blank check box means group members cannot perform that task. If a blank check box is greyed out, it means you cannot enable the task for the user group.
- The web GUI root and Monitor Lite groups, and the NBI groups, are not editable.
- Step 4** If you want to change permissions, you have these choices:
- Note** Be careful. Selecting and deselecting tasks in the Group Detail window will apply your changes to *all group members*.
- Change permissions for all user group members. See [View and Change the Tasks a Group Can Perform, on page 676](#).
  - Add the user to a different user group. The predefined user groups are described in [User Groups—Web UI, on page 672](#) and [User Groups—NBI, on page 673](#). Those topics also describe any group restrictions; for example, if a user belongs to the predefined Monitor Lite user group, the user cannot belong to any other groups.
  - Remove the user from this group. See [View and Change the Groups a User Belongs To, on page 674](#).
  - Use a customized user group and add the user to that group. To find out which customized groups already exist, see [View and Change the Tasks a Group Can Perform, on page 676](#). To create a new customized group, see [Create a Customized User Group, on page 675](#).
- 

## View and Change the Groups a User Belongs To

The tasks users can perform is determined by the user groups they belong to. This is normally configured when a user account is created (see [Add and Delete Users, on page 678](#)). User groups are described in [Types of User Groups, on page 672](#).



This procedure explains how to view the groups a user belongs to and, if necessary, change the user's group membership.

---

**Step 1** Choose **> Administration > Users, Roles & AAA Users**, then choose **Users**.

**Step 2** In the **User Name**, column, locate and click the user name hyperlink to open the **User Details** window. All user groups are listed under the General tab.

- A checked check box means the user belongs to that group. If a checked box is greyed-out, it means you cannot remove the user from that group. For example, Cisco EPN Manager will not allow you to remove the user named **root** from the root user group.
- A blank check box means the user does not belong to that group. If a blank check box is greyed-out, it means you cannot add the user to that group.

(To check the tasks that a group can perform, choose **User Groups** from the left sidebar menu and click a group name.)

**Step 3** To change the groups the user belongs to, select and unselect the appropriate groups in the **User Details** window, then click **Save**.

---

## View User Groups and Their Members

Users can belong to multiple groups, unless they belong to a very restricted group such as Monitoring Lite. This procedure explains how to view existing user groups and their members.

---

**Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **User Groups**.

The User Groups page lists all existing user groups and a short list of their members. For a description of these groups, see [Types of User Groups, on page 672](#).

**Step 2** To view all members of a group, click a group hyperlink to open the **Group Details** window, then click the **Members** tab.

**Step 3** If you want to make changes to these groups, see:

- [View and Change the Tasks a Group Can Perform, on page 676](#)
  - [View and Change the Groups a User Belongs To, on page 674](#)
- 

## Create a Customized User Group

Cisco EPN Manager provides a set of predefined user groups that help you control user authorization. These groups are described in [Types of User Groups, on page 672](#) and include four User Defined groups which you can customize to create a user group that is specific to your deployment. The following procedure explains how to create a customized group using one of the four predefined User Defined group templates.

---

**Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **User Groups**.

**Step 2** Locate a User Defined group that has no members, then click its group name hyperlink.

- Step 3** Customize the group permissions by checking and unchecking tasks in the **Group Detail** window. If a task is greyed-out, it means you cannot adjust its setting. You cannot change the group name.
- Step 4** Click **Save** to save your group settings.
- Step 5** Add members to your group by editing the relevant user accounts and adding the user to your new group. See [Add and Delete Users, on page 678](#) for information on adjusting user accounts.

## View and Change the Tasks a Group Can Perform

Follow these steps to get information about existing user groups and the tasks group members can perform. The predefined user groups are described in [View User Groups and Their Members, on page 675](#).



**Note** If you want to change *device* access, see [Assign Virtual Domains to Users, on page 687](#).

- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **User Groups**.  
The User Groups page lists all existing user groups.
- Step 2** Click a user group hyperlink. The **Group Detail** window lists the group permissions.
- A checked task means group members have permission to perform that task. If a checked box is greyed-out, it means you cannot disable the task.
  - A blank check box means group members cannot perform that task. If a blank check box is greyed out, it means you cannot enable the task for the user group.
- The web GUI root and Monitor Lite groups, and the NBI groups, are not editable.
- Step 3** If you want to change the group permissions—which will affect *all group members*—check and uncheck tasks, then click **Save**.
- Note** Be careful. Selecting and deselecting tasks in the Group Detail window will apply your changes to *all group members*. An alternative is to create a new group using one of the User Defined group templates; see [Create a Customized User Group, on page 675](#).

## Use Cisco EPN Manager User Groups with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the user groups that exist in Cisco EPN Manager. You can do this using the procedure in [Export the Cisco EPN Manager User Group and Task List Attributes for RADIUS and TACACS+, on page 676](#).

### Export the Cisco EPN Manager User Group and Task List Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all Cisco EPN Manager user group and task information into your Cisco Access Control Server (ACS) or Cisco Identity Services Engine (ISE) server. You can do this using the Task List dialog box provided in the Cisco EPN Manager web GUI. If you do not

export the data into your Cisco ACS or Cisco ISE server, Cisco EPN Manager will not allow users to perform their assigned tasks.

The following information must be exported, depending on the protocol you are using:

- TACACS+—Requires virtual domain, role, and task information.
- RADIUS—Requires virtual domain and role information (tasks are automatically added).

Information in the Task List dialog is preformatted for use with the Cisco ACS server.



**Note** When you add tasks to the external server, be sure to add the **Home Menu Access** task. It is mandatory for all users.

### Before you begin

Make sure you have added the AAA server and configured the AAA mode as explained in [Configure External Authentication, on page 691](#).

#### Step 1

In Cisco EPN Manager :

- Choose **Administration > Users > User Groups**.
- From the User Groups table, copy the tasks for each user group by clicking the **Task List** hyperlink (at the end of a user group row).
  - If you are using RADIUS, right-click *all of the text* in the RADIUS Custom Attributes field and choose **Copy**.
  - If you are using TACACS+, right-click *all of text* in the TACACS+ Custom Attributes field and choose **Copy**.

#### Step 2

Paste the information into your Cisco ACS or Cisco ISE server. These steps show how to add the information to an existing user group in Cisco ACS. If you have not yet added this information to Cisco ACS or Cisco ISE, see:

- [Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 697](#)
  - [Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 692](#)
- Navigate to **User or Group Setup**.
  - For the applicable user or group, click **Edit Settings**.
  - Paste the attributes list into the appropriate text box.
  - Select the check boxes to enable these attributes, then click **Submit + Restart**.

## Add Users and Manage User Accounts

- [Create Web GUI Users with Administrator Privileges, on page 678](#)
- [Add and Delete Users, on page 678](#)
- [Disable \(Lock\) a User Account, on page 679](#)
- [Change a User's Password, on page 679](#)

## Create Web GUI Users with Administrator Privileges

After installation, Cisco EPN Manager has a web GUI root account named **root**. This account is used for first-time login to the server to create:

- Web GUI users with Administrator privileges who will manage the product and features
- All other user accounts

You should *not* use the web GUI root account for normal operations. For security purposes, create a new web GUI user with Administrator privileges (and access to all devices), and then disable the web GUI root account.

- 
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **Users**.
- Step 2** From the **Select a command** drop-down list, choose **Add User**, then click **Go**.
- Step 3** Complete the required fields.
- Step 4** In the **General** tab under **Groups Assigned to This User**, click **Admin**.
- Step 5** Click the **Virtual Domains** tab to specify which devices the user can access. You should have at least one Admin web GUI user that has access to all devices (ROOT-DOMAIN). For more information on virtual domains, see [Create Virtual Domains to Control User Access to Devices, on page 682](#).
- Step 6** Click **Save**.
- 

### What to do next

If you have not done so already, for security purposes, disable the web GUI root account as described in [Disable and Enable the Web GUI root User, on page 671](#).

## Add and Delete Users

Before you create user accounts, create virtual domains to control device access so you can apply them during account creation. Otherwise you will have to edit the user account to add the domain access. See [Create Virtual Domains to Control User Access to Devices, on page 682](#).

If you want to temporarily disable an account (rather than delete it), see [Disable \(Lock\) a User Account, on page 679](#).

- 
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **Users**.
- Step 2** From the **Select a command** drop-down list, choose **Add User**, then click **Go**.
- Step 3** Configure the user account.
- Enter a username and password.
  - Enter the first name, last name, and a description for the user.
  - Control the actions the user can perform by selecting one or more user groups. For descriptions of user groups, see [View User Groups and Their Members, on page 675](#).
  - Control the devices a user can access by clicking the **Virtual Domains** tab and assigning domains to the user. (see [Create Virtual Domains to Control User Access to Devices, on page 682](#)).
- Step 4** Click **Save**.

- Step 5** To delete a user account, select a user, choose **Delete User** from the **Select a command** drop-down list, then click **Go**.
- 

## Disable (Lock) a User Account

Disable a user account when you temporarily want to disallow a user from logging in to the Cisco EPN Manager GUI. You might want to do this if a user is temporarily changing job functions. If the user tries to log in, Cisco EPN Manager displays a message saying the login failed because the account is locked. You can unlock the account later without having to re-create the user. If you want to delete a user account, see [Add and Delete Users, on page 678](#).

User accounts may be disabled automatically if the password is not changed before expiration. Only an administrator can reset the password in this case. See [Change a User's Password, on page 679](#) and [Configure Global Password Policies for Local Authentication, on page 681](#).

---

- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then click **Users**.
- Step 2** Select the user whose access you want to disable or enable.
- Step 3** From the **Select a command** drop-down list, select **Lock User(s)** (or **Unlock User(s)**), then click **Go**.
- 

## Change a User's Password

You can force users to change their passwords on a regular basis using password rules (see [Configure Global Password Policies for Local Authentication, on page 681](#)). Users can change their own passwords as described in [Change Your Password, on page 3](#). If you need to make an immediate change to a user's password, use this procedure.

---

- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then click **Users**.
- Step 2** Click the username hyperlink.
- Step 3** Enter the new password in the password fields, then click **Save**.
- 

## Find Out Which Users Are Currently Logged In

Use this procedure to find out who is currently logged into the Cisco EPN Manager server. You can also view a historical list of the actions performed by the user in the current web GUI session and past sessions.

---

- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **Active Sessions**. Cisco EPN Manager lists all users that are currently logged in to the Cisco EPN Manager server, including their client machine IP address. If the user performed any actions on managed devices (for example, the user added new devices to Cisco EPN Manager), the device IP addresses are listed in the Device IP Address column.
- Step 2** To view a historical list of all actions performed by this user, click the Audit Trail icon that corresponds to the user name.
-

## View the Tasks Performed By Users (Audit Trail)

Cisco EPN Manager maintains a history of all actions performed by users in active and past web GUI sessions. Follow these steps to view a historical list of tasks performed by a specific *user* or by all members of a specific *user group*. The audit information includes a description of the task, the IP address of the client from which the user performed the task, and the time at which the task was performed. If a task affects a managed device (for example, a user adds a new device), the affected device's IP address is listed in the Device IP Address column. If a change is made to multiple devices (for example, a user deploys a configuration template to 10 switches), Cisco EPN Manager displays an audit entry for each switch.

To find out which users are currently logged into the Cisco EPN Manager web GUI, see [Find Out Which Users Are Currently Logged In](#), on page 679.

To view audits that are not user-specific, see these topics:

- [Audit Actions Executed from the GUI \(System Audit\)](#), on page 719
- [Audit Configuration Archive and Software Management Changes \(Network Audit\)](#), on page 717
- [Audit Changes Made By Users \(Change Audit\)](#), on page 717

---

**Step 1** Choose **Administration > Users > Users, Roles & AAA**.

**Step 2** To view the tasks performed by a specific user:

1. Choose **Users**.
2. Locate the user name, then click the Audit Trail icon corresponding to that user.

**Step 3** To view a historical list of the tasks performed by all members of a user group:

1. Choose **User Groups**.
  2. Locate the user group name, then click the Audit Trail icon corresponding to that group.
- 

## Configure Job Approvers and Approve Jobs

Use job approval when you want to control jobs that could significantly impact the network. If a job requires approval, Cisco EPN Manager sends an e-mail to all users with Admin privileges and does not run the job until one of them approves it. If a job is rejected by an approver, the job is removed from the database. By default, all jobs do not require approval.

If job approval is already enabled and you want to view jobs that need approval, approve a job, or reject a job, choose **Administration > Settings > System Settings**, then choose **General > Job Approval**.

To enable job approval and configure the jobs that require approval before running:

---

**Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Job Approval**.

- Step 2** Check the **Enable Job Approval** check box.
- Step 3** Find the jobs you want to configure for approval, and move them from the left field to the right field. For example, if you want an Admin user to approve adding new devices, move the **Import job** type.
- Step 4** To specify a customized job type, enter a string using regular expressions in the Job Type field, then click **Add**. For example, to enable job approval for all job types that start with Config, enter **Config\***.
- Step 5** Click **Save**.
- 

## Configure Global Password Policies for Local Authentication

If you are using local authentication (Cisco EPN Manager's authentication mechanism), you control the global password policies from the web GUI. If you are authenticating Cisco EPN Manager users using external authentication, the policies are controlled by an external application (see [Set Up External Authentication Using the CLI, on page 607](#)).

By default, users are not forced to change passwords after any period of time. To enforce password changes and configure other password rules, choose **Administration > Users > Users, Roles & AAA**, then choose **Local Password Policy**.

## Configure the Global Timeout for Idle Users

Cisco EPN Manager provides two settings that control when and how idle users are automatically logged out:

- **User Idle Timeout**—You can disable or configure this setting, which ends your user session automatically when you exceed the timeout. It is enabled by default and is set to 15 minutes.
- **Global Idle Timeout**—The Global Idle Timeout setting overrides the User Idle Timeout setting. The Global Idle Timeout is enabled by default and is set to 15 minutes. Only users with administrative privileges can disable the Global Idle Timeout setting or change its time limit.

By default, client sessions are disabled and users are automatically logged out after 15 minutes of inactivity. This is a global setting that applies to all users. For security purposes, you should not disable this mechanism, but you can adjust the timeout value using the following procedure. To disable/change the timeout for an idle user, see [Disable Idle User Timeout, on page 682](#)

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Server**.
- Step 2** In the **Global Idle Timeout** area, make sure the **Logout all idle users** check box is selected (this means the mechanism is enabled).
- Step 3** Configure the timeout by choosing a value from the **Logout all idle users after** drop-down list.
- Step 4** Click **Save**. You will need to log out and log back in for this change to take effect.
-

## Disable Idle User Timeout

By default, client sessions are disabled and users are automatically logged out after certain period of inactivity. This is a global setting that applies to all users. To avoid being logged out during the installation, it is recommended to disable automatic logout of idle users in the system settings using the following procedure.



**Note** The Global Idle Timeout setting overrides the User Idle Timeout setting. To configure Global Idle Timeout settings, see [Configure the Global Timeout for Idle Users, on page 681](#).

**Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Server**.

**Step 2** In the **Global Idle Timeout** area, uncheck the **Logout all idle users** check box and click **Save**.

**Step 3** Click  at the top right of web GUI window and choose **My Preferences**.

**Step 4** In the **User Idle Timeout** area, uncheck the **Logout idle user** check box and click **Save**.

If you need to change the idle timeout value, then select **Logout idle user** check box and from the **Logout idle user after** drop-down list, choose one of the idle timeout limits. (But this cannot exceed the value set in the Global Idle Timeout settings.)

**Step 5** Click **Save**. You will need to log out and log back in for this change to take effect.

## Create Virtual Domains to Control User Access to Devices

- [What Are Virtual Domains?, on page 682](#)
- [How Virtual Domains Affect Cisco EPN Manager Features, on page 683](#)
- [Create New Virtual Domains, on page 684](#)
- [Import a List of Virtual Domains, on page 687](#)
- [Add Network Devices to Virtual Domains, on page 687](#)
- [Assign Virtual Domains to Users, on page 687](#)
- [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 689](#)
- [Edit a Virtual Domain, on page 688](#)
- [Delete a Virtual Domain, on page 688](#)

## What Are Virtual Domains?

Virtual domains are logical groupings of devices, sites, and other NEs, and are used to control who has access to those NEs. You choose which elements are included in a virtual domain and which users have access to that virtual domain. Virtual domains can be based on physical sites, device types, user communities, or any



other designation you choose. All devices belong to ROOT-DOMAIN, which is the parent domain for all new virtual domains.

Virtual domains work in conjunction with user groups. Virtual domains control the devices a user can access, while user groups determine the actions a user can perform on those devices. Users with access to a virtual domain (depending on their privileges) can configure devices, view alarms, and generate reports for the NEs in their virtual domain.

You can create virtual domains after you have added devices to Cisco EPN Manager . Each virtual domain must have a name and can have an optional description, email address, and time zone. Cisco EPN Manager uses the email address and time zone that you specify to schedule and email domain-specific reports.

Users work in one virtual domain at a time. Users can change the current virtual domain by choosing a different one from the Virtual Domain drop-down list (see [Work In a Different Virtual Domain , on page 24](#)).

Before you set up virtual domains, determine which users are responsible for managing particular areas of the network. Then organize your virtual domains according to those needs—for example, by geography, by device type, or by the user community served by the network.

## How Virtual Domains Affect Cisco EPN Manager Features

Virtual domains are organized hierarchically. The ROOT-DOMAIN domain includes all virtual domains.

Because network elements are managed hierarchically, user views of devices—as well as some associated features and components—are affected by the user's virtual domain. The following topics describe the effects of virtual domains on these features.

- [Reports and Virtual Domains, on page 683](#)
- [Search and Virtual Domains, on page 683](#)
- [Alarms and Virtual Domains, on page 684](#)
- [Maps and Virtual Domains, on page 684](#)
- [Configuration Templates and Virtual Domains, on page 684](#)
- [Config Groups and Virtual Domains, on page 684](#)
- [Email Notifications and Virtual Domains, on page 684](#)

### Reports and Virtual Domains

Reports only include components that belong to the active virtual domain. A parent virtual domain cannot view reports from its child domains. New components are only reflected in reports that are generated after the components were added.

### Search and Virtual Domains

Search results only include components that belong to the active domain. You can only view saved search results if you are in the same domain from which the search was performed and saved. When working in a parent domain, you cannot view the results of searches performed in child domains.

## Alarms and Virtual Domains

When a component is added to a virtual domain, no previous alarms for that component are visible to that virtual domain . Only new alarms are visible. For example, if a network element is added to Cisco EPN Manager , and that network element generated alarms before and after it was added, its alarm history would only include alarms generated after it was added.



### Note

For alarm email notifications, only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and Cisco EPN Manager email notifications.

## Maps and Virtual Domains

Maps only display network elements that are members of the active virtual domain.

## Configuration Templates and Virtual Domains

When you create or discover a configuration template in a virtual domain, it can only be applied to network elements in that virtual domain. If you apply a template to a device and then add that device to a child domain, the template is also available to the same device in the child domain.



### Note

If you create a child domain and then apply a configuration template to both network elements in the virtual domain, Cisco EPN Manager might incorrectly reflect the number of partitions to which the template was applied.

## Config Groups and Virtual Domains

A parent domain can view the network elements in a child domain's configuration groups. The parent domain can also edit the child domain's configuration groups.

## Email Notifications and Virtual Domains

Email notifications can be configured per virtual domain.

For *alarm* email notifications, only the ROOT-DOMAIN can enable Location Notifications, Location Servers, and email notifications.

## Create New Virtual Domains

To create a new virtual domain, use one of the following procedures depending on the desired hierarchy of the virtual domain.

| To create a new virtual domain ( <i>new-domain</i> ) here: | See this procedure:                                                            |
|------------------------------------------------------------|--------------------------------------------------------------------------------|
| ROOT-DOMAIN > <i>new-domain</i>                            | <a href="#">Create Virtual Domains Directly Under ROOT-DOMAIN, on page 685</a> |

|                                                                                          |                                                        |
|------------------------------------------------------------------------------------------|--------------------------------------------------------|
| ROOT-DOMAIN > <i>existing-domain</i> > <b><i>new-domain</i></b>                          | Create Child Virtual Domains (Subdomains), on page 685 |
| ROOT-DOMAIN > <i>existing-domain</i> > <i>existing-domain</i> > <b><i>new-domain</i></b> |                                                        |
| (etc.)                                                                                   |                                                        |

## Create Virtual Domains Directly Under ROOT-DOMAIN

The following procedure creates an empty virtual domain under ROOT-DOMAIN. You can also create multiple virtual domains at one time by using the procedure in [Import a List of Virtual Domains, on page 687](#).

If a virtual domain already exists under ROOT-DOMAIN, and you want to create a new domain under it (a child domain), see [Create Child Virtual Domains \(Subdomains\), on page 685](#).

- 
- Step 1** Choose **Administration > Users > Virtual Domains**.
- Step 2** In the Virtual Domains sidebar menu, click the + icon (Add New Domain).
- Step 3** Enter a name in the Name text box. This is required.
- Step 4** (Optional) Enter the new domain's time zone, email address and description.
- Step 5** Click **Submit** to view a summary of the newly-created virtual domain.
- 

### What to do next

Add devices to the virtual domain as described in [Add Network Devices to Virtual Domains, on page 687](#).

## Create Child Virtual Domains (Subdomains)

The following procedure creates a child virtual domain (also called a subdomain). A child virtual domain is a domain that is *not* directly under ROOT-DOMAIN; it is under a domain that is under ROOT-DOMAIN.

Do not use this procedure if you want the new virtual domain to appear directly under ROOT-DOMAIN. In that case, see [Create Virtual Domains Directly Under ROOT-DOMAIN, on page 685](#).

- 
- Step 1** Choose **Administration > Users > Virtual Domains**.
- Step 2** In the Virtual Domains sidebar menu:
- Locate the domain under which you want to create a new child domain. (This is called the parent domain.) In this example, the parent domain is **California**.
  - Click the information (i) icon next to the domain name. This opens a data popup window.
  - In the popup window, click **Create Sub Domain**. The navigation pane switches to the list view, with the parent domain **California** displayed above **Untitled**.
- Step 3** Enter a name in the Name text box. This is required. In this example, the new child domain is named **Los Angeles**. (The name in the navigation pane will not change from **Untitled** to **Los Angeles** until you save the new child domain.)

## Create Child Virtual Domains (Subdomains)

ROOT-DOMAIN  
Untitled

\* Name  Time Zone  Parent Domain

Email Address  Description

Site Maps Groups **Network Devices** Access Points Virtual Elements

Selected Network Devices By Groups

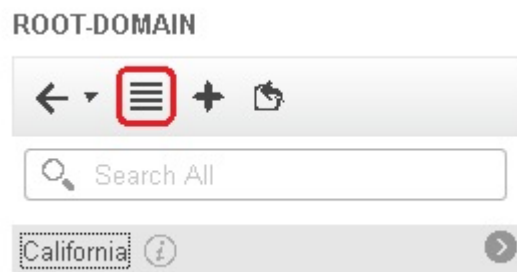
Selected Network Devices

+ Add X Delete

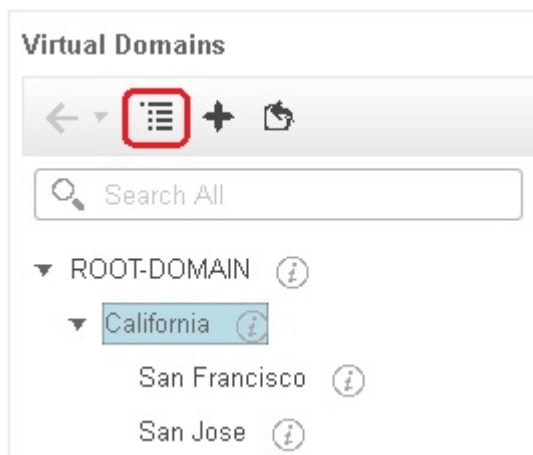
| <input type="checkbox"/> | Device Name          | IP Address/DNS       | Device               |
|--------------------------|----------------------|----------------------|----------------------|
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

**Step 4** (Optional) Enter the new domain's time zone, email address and description.

**Step 5** Click **Submit** and confirm the creation of the new child domain. To revert back to the hierarchical view, click the view toggle button at the top of the navigation pane.



The view reverts to the hierarchical view.



### What to do next

Add devices to the virtual domain as described in [Add Network Devices to Virtual Domains, on page 687](#).

## Import a List of Virtual Domains

If you plan to create many virtual domains, or give them a complex hierarchy, you will find it easier to specify them in a properly formatted CSV file, and then import it. The CSV format allows you to specify a name, description, time zone, and email address for each virtual domain you create, as well as each domain's parent domain. Adding network elements to the virtual domains must be performed separately.

- 
- Step 1** Choose **Administration > Users > Virtual Domains**.
  - Step 2** Click the **Import Domain(s)** icon, download a sample CSV file from the link provided in the popup, and prepare the CSV file.
  - Step 3** Click **Choose File** and navigate to your CSV file.
  - Step 4** Click **Import** to import the CSV and create the virtual domains you specified.
- 

### What to do next

Add devices to the virtual domains as explained in [Add Network Devices to Virtual Domains, on page 687](#).

## Add Network Devices to Virtual Domains

Use this procedure to add network devices to a virtual domain. When you add a new network device to an existing virtual domain, the device becomes immediately accessible to users with access to that domain (users do not have to restart the web GUI).

- 
- Step 1** Choose **Administration > Users > Virtual Domains**.
  - Step 2** From the Virtual Domains sidebar menu, click the virtual domain to which you want to add network devices.
  - Step 3** Click the **Network Devices** tab, then click **Add**.
  - Step 4** Select the network devices you want to add to the domain. Note that the Select Network Devices dialog lists all managed devices, not only those that are in the parent domain. If you add a device that is not included in the parent domain, Cisco EPN Manager adds it to both the child and parent domain.
    - a) Select the devices you want to add to the domain. You can use the **Filter By** drop-down list to locate the devices you want to add.
    - b) Click **Select**.
  - Step 5** Click **Submit** to view the summary of the virtual domain contents.
  - Step 6** Click **Save** to confirm your changes.
- 

### What to do next

Give users access to the virtual domain as described in [Assign Virtual Domains to Users, on page 687](#).

## Assign Virtual Domains to Users

Once a virtual domain is assigned to a user account, the user is restricted to viewing and performing operations on the devices in their assigned domain(s).



**Note** When using external AAA, be sure to add the custom attributes for virtual domains to the appropriate user or group configuration on the external AAA server. See [Use Cisco EPN Manager Virtual Domains with RADIUS and TACACS+, on page 689](#).

- 
- Step 1** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 2** Select the user to whom you want to grant device access.
- Step 3** Click the **Virtual Domains** tab.
- Step 4** Use the **Add** and **Remove** buttons to make your assignment changes, then click **Save**.
- 

## Edit a Virtual Domain

To adjust a virtual domain, choose it from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned network devices. You cannot edit any of the settings for ROOT-DOMAIN.

- 
- Step 1** Choose **Administration > Users > Virtual Domains**.
- Step 2** Click the virtual domain you want to edit in the Virtual Domains sidebar menu.
- Step 3** To adjust the name, email address, time zone, or description, enter your changes in the text boxes.
- Step 4** To adjust device members:
- To add devices, click **Add** and follow the instructions in [Add Network Devices to Virtual Domains, on page 687](#).
  - To delete devices, select the devices using their check boxes, then click **Delete**.
- Step 5** Click **Submit**, then check the summary of your changes.
- Step 6** Click **Save** to apply and save your edits.
- 

## Delete a Virtual Domain

Use this procedure to delete a virtual domain from Cisco EPN Manager . This procedure only deletes the virtual domain; it does not delete the network elements from Cisco EPN Manager (the network elements will continue to be managed by Cisco EPN Manager ).

### Before you begin

You can only delete a virtual domain if:

- The virtual domain does not contain any network elements and does not have any child domains.
- It is not the only domain a user can access. In other words, if a Cisco EPN Manager user has access to *only* that domain, you cannot delete it.
- No users are logged into the domain.

- 
- Step 1** Choose **Administration > Users > Virtual Domains**.
- Step 2** In the Virtual Domains sidebar menu, click the information (i) icon next to the virtual domain name. This opens a data popup window.
- Step 3** In the popup window, click **Delete**.
- Step 4** Click **OK** to confirm deleting the virtual domain.
- 

## Use Cisco EPN Manager Virtual Domains with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the virtual domains that exist in Cisco EPN Manager. You can do this using the procedure in [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 689](#).

If your RADIUS or TACACS+ server does not have any virtual domain information for a user, the following occurs, depending on the number of virtual domains that are configured in Cisco EPN Manager :

- If Cisco EPN Manager has only one virtual domain (ROOT-DOMAIN), the user is assigned the ROOT-DOMAIN by default.
- If Cisco EPN Manager has multiple virtual domains, the user is prevented from logging in.

## Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all Cisco EPN Manager virtual domain information into your Cisco ACS or Cisco ISE server. You can do this using the Virtual Domains Custom Attributes dialog box provided in the Cisco EPN Manager web GUI. If you do not export the data into your Cisco ACS or Cisco ISE server, Cisco EPN Manager will not allow users to log in.

The following information must be exported, depending on the protocol you are using:

- TACACS+—Requires virtual domain, role, and task information.
- RADIUS—Requires virtual domain and role information (tasks are automatically added).

When you create a child domain for an existing virtual domain, the sequence numbers for the RADIUS/TACACS+ custom attributes are also updated in the parent virtual domain. These sequence numbers are for representation only and do not impact AAA integration.

Information in the Virtual Domains Custom Attributes dialog is preformatted for use with Cisco ACS server.



---

**Note** When you add tasks to the external server, be sure to add the **Home Menu Access** task. It is mandatory for all users.

---

### Before you begin

Make sure you have added the AAA server and configured the AAA mode as explained in [Configure External Authentication, on page 691](#).

- 
- Step 1** In Cisco EPN Manager :
- Choose **Administration > Users > Virtual Domains**.
  - Click **Export Custom Attributes** at the top right of the window. This opens the Virtual Domain Custom Attributes dialog.
  - Copy the attributes list.
    - If you are using RADIUS, right-click *all of the text* in the RADIUS Custom Attributes field and choose **Copy**.
    - If you are using TACACS+, right-click *all of text* in the TACACS+ Custom Attributes field and choose **Copy**.
- Step 2** Paste the information into your Cisco ACS or Cisco ISE server. These steps show how to add the information to an existing user group in Cisco ACS. If you have not yet added this information to Cisco ACS or Cisco ISE, see:
- [Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 697](#)
  - [Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 692](#)
- Navigate to **User or Group Setup**.
 

If you want to specify virtual domains on a per-user basis, then you need to make sure you add all of the custom attributes (for example, tasks, roles, virtual domains) information to the User custom attribute page.
  - For the applicable user or group, click **Edit Settings**.
  - Paste the attributes list into the appropriate text box.
  - Select the check boxes to enable these attributes, then click **Submit + Restart**.
- 

## Configure Local Authentication

Cisco EPN Manager uses local authentication by default, which means that user passwords are stored and verified from the Cisco EPN Manager database. To check the authentication mode that is being used, choose **Administration > Users > Users, Roles & AAA**, then choose **AAA Mode Settings**. The selection is displayed on the AAA Mode Settings page. If you are using local authentication, be sure to configure strong password policies. See [Configure Global Password Policies for Local Authentication, on page 681](#).

If you want to use SSO with local authentication, see [Use SSO With Local Authentication, on page 690](#).

For information on external authentication, see [Configure External Authentication, on page 691](#).

## Use SSO With Local Authentication

To use SSO with local authentication, you must add the SSO server and then configure Cisco EPN Manager to use SSO in local mode.

If you have deployed Cisco EPN Manager in a high availability environment where you have a primary and backup server, refer to the instructions in [Configure an SSO Server in an HA Environment, on page 731](#).

Cisco EPN Manager does not support localization on the SSO sign-in page.

The following topics describe how to configure SSO for external authentication, but you can use the same procedures to configure SSO for local authentication. The only difference is that when you configure the SSO mode on the Cisco EPN Manager server, choose **Local** mode (not RADIUS or TACACS+).



- [Add the SSO Server, on page 703](#)
- [Configure SSO Mode on the Cisco EPN Manager Server, on page 703](#)

## Configure External Authentication

Users with web GUI root user or SuperUser privileges can configure Cisco EPN Manager to communicate with external RADIUS, TACACS+, and SSO servers for external authentication, authorization, and accounting (AAA). If you choose to configure external authentication, the user groups, users, authorization profiles, authentication policies, and policy rules must be created in the external server through which all access requests to Cisco EPN Manager will be routed.

You can use a maximum of three AAA servers. Users are authenticated on the second server only if the first server is not reachable or has network problems.

If you want to configure external authentication from the CLI, see [Set Up External Authentication Using the CLI, on page 607](#).

See the following topics for more information.

- [Use RADIUS or TACACS+ for External Authentication, on page 691](#)
- [Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 692](#)
- [Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 697](#)
- [Use SSO with External Authentication, on page 703](#)

## Use RADIUS or TACACS+ for External Authentication

These topics explain how to configure Cisco EPN Manager to use RADIUS or TACACS+ servers.

- [Add a RADIUS or TACACS+ Server to Cisco EPN Manager , on page 691](#)
- [Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server, on page 692](#)

### Add a RADIUS or TACACS+ Server to Cisco EPN Manager

To add a RADIUS or TACACS+ server to Cisco EPN Manager :

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Administration &gt; Users &gt; Users, Roles &amp; AAA</b> , then choose <b>RADIUS Servers</b> .                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 2</b> | Select the type of server you want to add. <ul style="list-style-type: none"><li>• For RADIUS, choose <b>RADIUS Servers</b>. From the <b>Select a command</b> drop-down list, choose <b>Add RADIUS Server</b>, then click <b>Go</b>.</li><li>• For TACACS+, choose <b>TACACS+ Servers</b>. From the <b>Select a command</b> drop-down list, choose <b>Add TACACS+ Server</b>, then click <b>Go</b>.</li></ul>                                           |
| <b>Step 3</b> | Enter the required information—IP address, DNS Name, and so forth. For Cisco EPN Manager to communicate with the external authentication server, the shared secret you enter on this page must match the shared secret configured on the RADIUS or TACACS+ server. You can use alphabets, numbers, and special characters except ‘ (single quote) and “ (double quote) while entering the shared secret key for a third-party TACACS+ or RADIUS server. |
| <b>Step 4</b> | Select the authentication type.                                                                                                                                                                                                                                                                                                                                                                                                                         |

- PAP—Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication.
- CHAP—Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

**Step 5** If you have enabled the High Availability feature and configured a virtual IP address for the **Local Interface IP**, choose either the virtual IP address or the physical IP address of the primary server. . (See the information on setting up and installing high availability on a secondary server in the [Cisco Evolved Programmable Network Manager Installation Guide](#).)

**Note** The IP address configured in the external authentication server must match the **Local Interface IP**.

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

## Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server

**Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **AAA Mode**.

**Step 2** Select **TACACS+** or **RADIUS**.

**Step 3** Check the **Enable Fallback to Local** check box to enable the use of the local database when the external AAA server is down.

**Step 4** If you want to revert to local authentication if the external RADIUS or TACACS+ server goes down, perform the following steps:

- Select **Enable Fallback to Local**. I
- Specify the fall back conditions—either **ONLY on no server response** or **on authentication failure or no server response**.

**Step 5** Click **Save**.

## Use Cisco ISE With RADIUS or TACACS+ for External Authentication

Cisco Identity Services Engine (ISE) uses the RADIUS or TACACS+ protocols for authentication, authorization, and accounting (AAA). You can integrate Cisco EPN Manager with Cisco ISE to authenticate the Cisco EPN Manager users using the RADIUS or TACACS+ protocols. When you use external authentication, the details such as users, user groups, passwords, authorization profiles, authorization policies, and policy rules that are required for AAA must be stored and verified from the Cisco ISE database.

Complete the following tasks to use Cisco ISE with the RADIUS or TACACS+ protocol for external authentication:

| Tasks to be completed to use Cisco ISE for external authentication | For information, see:                                                              |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Make sure you are using a supported version of Cisco ISE           | <a href="#">Supported Versions of Cisco ISE in Cisco EPN Manager</a> , on page 693 |

|                                                                                                                                                                                                                                                                                                                                     |                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Add Cisco EPN Manager as an AAA client in Cisco ISE                                                                                                                                                                                                                                                                                 | <a href="#">Add Cisco EPN Manager as a Client in Cisco ISE, on page 693</a>                   |
| Create a user group in Cisco ISE                                                                                                                                                                                                                                                                                                    | <a href="#">Create a User Group in Cisco ISE, on page 694</a>                                 |
| Create a user in Cisco ISE and add the user to the user group that is created in Cisco ISE                                                                                                                                                                                                                                          | <a href="#">Create a User and Add the User to a User Group in Cisco ISE, on page 694</a>      |
| (If using RADIUS) Create an authorization profile for network access in Cisco ISE, and add the RADIUS custom attributes with user roles and virtual domains created in Cisco EPN Manager<br><br><b>Note</b> For RADIUS, you do not need to add the attributes for user tasks. They are automatically added based on the user roles. | <a href="#">Create an Authorization Profile for RADIUS in Cisco ISE, on page 694</a>          |
| (If using TACACS+) Create an authorization profile for network access in Cisco ISE, and add the TACACS+ custom attributes with user roles, tasks, and virtual domains created in Cisco EPN Manager<br><br><b>Note</b> For TACACS+, you must also add the attributes for user tasks.                                                 | <a href="#">Create an Authorization Profile for TACACS+ in Cisco ISE, on page 695</a>         |
| Create an authorization policy in Cisco ISE and associate the policy with the user groups and authorization profile created in Cisco ISE                                                                                                                                                                                            | <a href="#">Configure an Authorization Policy in Cisco ISE, on page 696</a>                   |
| Create an authentication policy to define the protocols that Cisco ISE must use to communicate with Cisco EPN Manager, and the identity sources that it uses for authenticating users to Cisco EPN Manager                                                                                                                          | <a href="#">Create an Authentication Policy in Cisco ISE, on page 697</a>                     |
| Add Cisco ISE as a RADIUS or TACACS+ server in Cisco EPN Manager                                                                                                                                                                                                                                                                    | <a href="#">Add a RADIUS or TACACS+ Server to Cisco EPN Manager, on page 691</a>              |
| Configure the RADIUS or TACACS+ mode on the Cisco EPN Manager server                                                                                                                                                                                                                                                                | <a href="#">Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server, on page 692</a> |

## Supported Versions of Cisco ISE in Cisco EPN Manager

Cisco EPN Manager supports Cisco ISE 1.x and 2.x releases.

### Add Cisco EPN Manager as a Client in Cisco ISE

- 
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Administration > Network Resources > Network Devices**.
- Step 3** In the **Network Devices** page, click **Add**.
- Step 4** Enter the device name and IP address of the Cisco EPN Manager server.
- Step 5** Check the **Authentication Settings** check box, and then enter the shared secret.

**Note** Ensure that this shared secret matches the shared secret you enter when adding the Cisco ISE server as the RADIUS server in Cisco EPN Manager .

**Step 6** Click **Submit**.

---

## Create a User Group in Cisco ISE

---

- Step 1** Log in to Cisco ISE as the admin user.
  - Step 2** Choose **Administration > Identity Management > Groups**.
  - Step 3** In the **User Identity Groups** page, click **Add**.
  - Step 4** In the **Identity Group** page, enter the name and description of the user group.
  - Step 5** Click **Submit**.
- 

## Create a User and Add the User to a User Group in Cisco ISE

---

- Step 1** Log in to Cisco ISE as the admin user.
  - Step 2** Choose **Administration > Identity Management > Identities**.
  - Step 3** In the **Network Access Users** page, click **Add**.
  - Step 4** From the **Select an item** drop-down list, choose a user group to assign the user to.
  - Step 5** Click **Submit**.
- 

## Create an Authorization Profile for RADIUS in Cisco ISE

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the RADIUS custom attributes that are associated with user roles, tasks, and virtual domains created in Cisco EPN Manager .



**Note** For RADIUS, you can add the user role attributes without adding the task attributes. The tasks are automatically added with the user roles.

---

For more information about Cisco ISE authorization profiles, see the information on managing authorization policies and profiles in the [Cisco Identity Services Engine Administrator Guide](#).

To create an authorization profile for RADIUS in Cisco ISE:

**Before you begin**

Make sure you have the complete list of the following Cisco EPN Manager custom attributes for RADIUS. You will need to add this information to Cisco ISE in this procedure.

- Cisco EPN Manager user roles and tasks—see [Export the Cisco EPN Manager User Group and Task List Attributes for RADIUS and TACACS+, on page 676](#)
- Cisco EPN Manager virtual domains—see [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 689](#)

- 
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Policy > Policy Elements > Results**.
- Step 3** From the left sidebar, choose **Authorization > Authorization Profiles**.
- Step 4** In the **Standard Authorization Profiles** page, click **Add**.
- Step 5** In the **Authorization Profile** page, enter the name and description of the authorization profile.
- Step 6** From the **Access Type** drop-down list, choose **ACCESS\_ACCEPT**.
- Step 7** In the **Advanced Attributes Settings** area, paste in the complete list of RADIUS custom attributes for:
- User roles
  - Virtual domains
- Note** If you do add user tasks, be sure to add the Home Menu Access task. It is mandatory.
- Step 8** Click **Submit**.
- 

## Create an Authorization Profile for TACACS+ in Cisco ISE

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the TACACS+ custom attributes that are associated with user roles, tasks, and virtual domains created in Cisco EPN Manager .



**Note** For TACACS+, you must add the user role *and* task attributes. (Task attributes are not required for RADIUS.)

For more information about Cisco ISE authorization profiles, see the information on managing authorization policies and profiles in the [Cisco Identity Services Engine Administrator Guide](#).

To create an authorization profile for TACACS+ in Cisco ISE:

**Before you begin**

Make sure you have the complete list of the following Cisco EPN Manager custom attributes for TACACS+. You will need to add this information to Cisco ISE in this procedure.

- Cisco EPN Manager user roles and tasks—see [Export the Cisco EPN Manager User Group and Task List Attributes for RADIUS and TACACS+, on page 676](#)

- Cisco EPN Manager virtual domains—see [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 689](#)

- 
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Policy > Policy Elements > Results**.
- Step 3** From the left sidebar, choose **Authorization > Authorization Profiles**.
- Step 4** In the **Standard Authorization Profiles** page, click **Add**.
- Step 5** In the **Authorization Profile** page, enter the name and description of the authorization profile.
- Step 6** From the **Access Type** drop-down list, choose **ACCESS\_ACCEPT**.
- Step 7** In the **Advanced Attributes Settings** area, paste in the complete list of TACACS+ custom attributes for:
- User roles, including the tasks
  - Virtual domains
- Note** Be sure to add the Home Menu Access task. It is mandatory.
- Step 8** Click **Submit**.
- 

## Configure an Authorization Policy in Cisco ISE

An authorization policy consists of a rule or a set of rules that are user-defined and produce a specific set of permissions, which are defined in an authorization profile. Based on the authorization profile, access requests to Cisco EPN Manager are processed.

There are two types of authorization policies that you can configure:

- **Standard**—Standard policies are intended to be stable and are created to remain in effect for long periods of time, to apply to a larger group of users, devices, or groups that share a common set of privileges.
- **Exception**—Exception policies are created to meet an immediate or short-term need, such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users.

For more information about authorization policies, see the “Manage Authorization Policies and Profiles” chapter in the [Cisco Identity Services Engine Administrator Guide](#).

To create an authorization policy in Cisco ISE:

- 
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Policy > Authorization**.
- Step 3** In the **Standard** area, click the down arrow on the far right and select either **Insert New Rule Above** or **Insert New Rule Below**.
- Step 4** Enter the rule name and choose identity group, condition, attribute, and permission for the authorization policy.
- For example, you can define a user group as Cisco EPN Manager -SystemMonitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as Cisco EPN Manager -SystemMonitoring-authorization profile and choose this profile from the Permissions drop-down list. Now, you have

defined a rule where all users belonging to the Cisco EPN Manager System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.

**Step 5** Click **Done**, and then click **Save**.

---

## Create an Authentication Policy in Cisco ISE

Authentication policies define the protocols that Cisco ISE uses to communicate with Cisco EPN Manager , and the identity sources that it uses for authenticating users to Cisco EPN Manager . An identity source is an internal or external database where the user information is stored.

You can create two types of authentication policies in Cisco ISE:

- Simple authentication policy - In this policy, you can choose the allowed protocols and identity sources to authenticate users.
- Rule-based authentication policy - In this policy, you can define conditions that allow Cisco ISE to dynamically choose the allowed protocols and identity sources.

For more information about authentication policies, see the "Manage Authentication Policies" chapter in the [Cisco Identity Services Engine Administrator Guide](#).

To create an authentication policy in Cisco ISE:

- 
- Step 1** Log in to Cisco ISE as the Super Admin or System Admin user.
- Step 2** Choose **Policy > Authentication**.
- Step 3** Choose the Policy Type as **Simple** or **Rule-Based** to create the required authentication policy.
- Step 4** Enter the required details based on the policy type selected.
- Step 5** Click **Save**.
- 

## Use Cisco ACS With RADIUS or TACACS+ for External Authentication

Cisco Secure Access Control System (ACS) uses RADIUS and TACACS+ protocol for authentication, authorization, and accounting (AAA). You can integrate Cisco EPN Manager with Cisco ACS to authenticate the Cisco EPN Manager users using the RADIUS or TACACS+ protocol. When you use an external authentication, the details such as users, user roles, passwords, authorization profiles, authorization policies, and policy rules that are required for AAA must be stored and verified from the Cisco ACS database.

Complete the following tasks to use Cisco ACS with the RADIUS or TACACS+ protocol for external authentication:

| Tasks to be completed to use Cisco ACS for external authentication | For information, see:                                                              |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Make sure you are using a supported version of Cisco ACS           | <a href="#">Supported Versions of Cisco ACS in Cisco EPN Manager , on page 698</a> |
| Add Cisco EPN Manager as an AAA client in Cisco ACS                | <a href="#">Add Cisco EPN Manager as a Client in Cisco ACS, on page 698</a>        |

|                                                                                                                                                                                                                                                                                                                                      |                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Create a user group in Cisco ACS                                                                                                                                                                                                                                                                                                     | <a href="#">Create a User Group in Cisco ACS, on page 699</a>                                 |
| Create a user in Cisco ACS and add the user to the Cisco ACS user group                                                                                                                                                                                                                                                              | <a href="#">Create a User and Add the User to a User Group in Cisco ACS, on page 699</a>      |
| (If using RADIUS) Create an authorization profile for network access in Cisco ACS, and add the RADIUS custom attributes for user roles and virtual domains created in Cisco EPN Manager .<br><br><b>Note</b> For RADIUS, you do not need to add the attributes for user tasks. They are automatically added based on the user roles. | <a href="#">Create an Authorization Profile for RADIUS in Cisco ACS, on page 699</a>          |
| (If using TACACS+) Create an authorization profile for device administration in Cisco ACS, and add the TACACS+ custom attributes with user roles, tasks, and virtual domains created in Cisco EPN Manager .<br><br><b>Note</b> For TACACS+, you must also add the attributes for user tasks.                                         | <a href="#">Create an Authorization Profile for TACACS+ in Cisco ACS, on page 700</a>         |
| Create an access service in Cisco ACS and define a policy structure for the access service.                                                                                                                                                                                                                                          | <a href="#">Create an Access Service for Cisco EPN Manager in Cisco ACS, on page 701</a>      |
| Create an authorization policy rule in Cisco ACS, and map the authorization or shell profile based on the access type (network access or device administration).                                                                                                                                                                     | <a href="#">Create an Authorization Policy Rule in Cisco ACS, on page 702</a>                 |
| Configure a service selection policy in Cisco ACS and assign an access service to an incoming request.                                                                                                                                                                                                                               | <a href="#">Configure a Service Selection Policy in Cisco ACS, on page 702</a>                |
| Add Cisco ACS as a RADIUS or TACACS+ server in Cisco EPN Manager .                                                                                                                                                                                                                                                                   | <a href="#">Add a RADIUS or TACACS+ Server to Cisco EPN Manager , on page 691</a>             |
| Configure the RADIUS or TACACS+ mode on the Cisco EPN Manager server.                                                                                                                                                                                                                                                                | <a href="#">Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server, on page 692</a> |

## Supported Versions of Cisco ACS in Cisco EPN Manager

Cisco EPN Manager supports Cisco ACS 5.x releases.

## Add Cisco EPN Manager as a Client in Cisco ACS

- 
- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Network Resources > Network Devices > Network Devices and AAA Clients**.
- Step 3** In the **Network Devices** page, click **Create**.



- Step 4** Enter the device name and IP address of the Cisco EPN Manager server.
- Step 5** Choose the authentication option as **RADIUS** or **TACACS+**, and enter the shared secret.
- Note** Ensure that this shared secret matches the shared secret you enter when adding the Cisco ACS server as the RADIUS or TACACS+ server in Cisco EPN Manager .
- Step 6** Click **Submit**.
- 

## Create a User Group in Cisco ACS

---

- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, Choose **Users and Identity Stores > Identity Groups**.
- Step 3** In the **Identity Groups** page, click **Create**.
- Step 4** Enter the name and description of the user group.
- Step 5** Select a network device group parent for the user group.
- Step 6** Click **Submit**.
- 

## Create a User and Add the User to a User Group in Cisco ACS

---

- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, Choose **Users and Identity Stores > Internal Identity Stores > Users**.
- Step 3** In the **Internal Users** page, click **Create**.
- Step 4** Enter the required details.
- Step 5** In the **Identity Group** field, click **Select** to choose a user group to assign the user to.
- Step 6** Click **Submit**.
- 

## Create an Authorization Profile for RADIUS in Cisco ACS

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the RADIUS custom attributes that are associated with user roles, tasks, and virtual domains created in Cisco EPN Manager .



**Note** For RADIUS, you can add the user role attributes without adding the task attributes. The tasks are automatically added with the user roles.

For more information about Cisco ACS authorization profiles and policies, see chapters on managing policy elements and access policies in the [User Guide for Cisco Secure Access Control System](#).

To create an authorization profile for RADIUS in Cisco ACS:

### Before you begin

Make sure you have the complete list of the following Cisco EPN Manager custom attributes for RADIUS. You will need to add this information to Cisco ACS in this procedure.

- Cisco EPN Manager user roles and tasks—see [Export the Cisco EPN Manager User Group and Task List Attributes for RADIUS and TACACS+, on page 676](#)
- Cisco EPN Manager virtual domains—see [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 689](#)

- 
- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Policy Elements > Authorizations and Permissions > Network Access > Authorization Profiles**.
- Step 3** Click **Create**.
- Step 4** On the **General** tab, enter the name and description of the authorization profile.
- Step 5** Click the **RADIUS Attributes** tab, and paste in the complete list of RADIUS custom attributes for:
- User roles
  - Virtual domains
- Note** If you do add user tasks, be sure to add the Home Menu Access task. It is mandatory.
- Step 6** Click **Submit**.
- 

## Create an Authorization Profile for TACACS+ in Cisco ACS

When you create an authorization profile for device administration, you must add the TACACS+ custom attributes that are associated with user roles, tasks, and virtual domains created in Cisco EPN Manager .



**Note** For TACACS+, you must add the user role *and* task attributes. (Task attributes are not required for RADIUS.)

For more information about Cisco ACS authorization profiles and policies, see chapters on managing policy elements and access policies in the [User Guide for Cisco Secure Access Control System](#).

To create an authorization profile for TACACS+ in Cisco ACS:

### Before you begin

Make sure you have the complete list of the following Cisco EPN Manager custom attributes. You will need to add this information to Cisco ACS in this procedure.

- Cisco EPN Manager user roles and tasks—see [Export the Cisco EPN Manager User Group and Task List Attributes for RADIUS and TACACS+, on page 676](#)
- Cisco EPN Manager virtual domains—see [Export the Cisco EPN Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 689](#).

- 
- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Policy Elements > Authorizations and Permissions > Device Administration > Shell Profiles**.
- Step 3** Click **Create**.
- Step 4** On the **General** tab, enter the name and description of the authorization profile.
- Step 5** Click the **Custom Attributes** tab, and paste in the complete list of TACACS+ custom attributes for:
- User roles, including the tasks
  - Virtual domains
- Step 6** Click **Submit**.
- 

## Create an Access Service for Cisco EPN Manager in Cisco ACS

Access services contain the authentication and authorization policies for access requests. You can create separate access services for different use cases; for example, device administration (TACACS+), network access (RADIUS), and so on.

When you create an access service in Cisco ACS, you define the type of policies and policy structures that it contains; for example, policies for device administration, network access, and so on.



---

**Note** You must create access services before you define service selection rules, although you do not need to define the policies in the services.

---

To create an access service for Cisco EPN Manager requests:

- 
- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Access Policies > Access Services**.
- Step 3** Click **Create**.
- Step 4** Enter the name and description of the access service.
- Step 5** Choose one of the following options to define a policy structure for the access service:
- **Based on service template**—Creates an access service containing policies based on a predefined template.
  - **Based on existing service**—Creates an access service containing policies based on an existing access service. However, the new access service does not include the existing service's policy rules.
  - **User selected service type**—Provides you the option to select the access service type. The available options are Network Access (RADIUS), Device Administration (TACACS+), and External Proxy (External RADIUS or TACACS+ servers).
- Step 6** Click **Next**.
- Step 7** Choose the authentication protocols that are allowed for the access service.
- Step 8** Click **Finish**.
-

## Create an Authorization Policy Rule in Cisco ACS

- 
- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Access Policies > Access Services > service > Authorization**.
- Step 3** Click **Create**.
- Step 4** Enter the name of the rule and then choose the rule status.
- Step 5** Configure the required conditions for the rule.
- For example, you can create a rule based on the location, device type, or user group that you have created.
- Step 6** If you are creating an authorization policy rule for network access (RADIUS), choose the required authorization profile(s) to map to the authorization policy rule.
- Alternatively, if you are creating an authorization policy rule for device administration (TACACS+), choose the required shell profile(s) to map to the authorization policy rule.
- Note** If you are using multiple authorization profiles or shell profiles, make sure you order them in priority.
- Step 7** Click **OK**.
- 

## Configure a Service Selection Policy in Cisco ACS

A service selection policy determines which access service applies to an incoming request. For example, you can configure a service selection policy to apply the device administration access service to any access request that uses the TACACS+ protocol.

You can configure two types of service selection policy:

- Simple service selection policy—Applies the same access service to all requests.
- Rule-based service selection policy—Contains one or more conditions and a result, which is the access service that will be applied to an incoming request.

To configure a service selection policy:

- 
- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Access Policies > Access Services > Service Selection Rules**.
- Step 3** If you want to configure a simple service selection policy, click the **Single result selection** radio button, and then choose an access service to apply to all requests.
- Alternatively, if you want to configure a rule-based service selection policy, click the **Rule based result selection** radio button, and then click **Create**.
- Step 4** Enter the name of the rule and then choose the rule status.
- Step 5** Choose either **RADIUS** or **TACACS+** as the protocol for the service selection policy.
- Step 6** Configure the required compound condition, and then choose an access service to apply to an incoming request.
- Step 7** Click **OK**, and then click **Save Changes**.
-

## Use SSO with External Authentication

To set up and use SSO (with or without a RADIUS or TACACS+ server), see these topics:

- [Add the SSO Server, on page 703](#)
- [Configure SSO Mode on the Cisco EPN Manager Server, on page 703](#)

Cisco EPN Manager does not support localization on the SSO sign-in page.

### Add the SSO Server

If you have deployed Cisco EPN Manager in a high availability environment where you have a primary and backup server, refer to the instructions in [Configure an SSO Server in an HA Environment, on page 731](#).

Cisco EPN Manager can be configured with a maximum of three AAA servers.

- 
- |               |                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Administration &gt; Users &gt; Users, Roles &amp; AAA</b> , then choose <b>SSO Servers</b> .         |
| <b>Step 2</b> | From the <b>Select a command</b> drop-down list, choose <b>Add SSO Servers</b> , then click <b>Go</b> .        |
| <b>Step 3</b> | Enter the SSO information. The maximum number of server retries for an SSO server authentication request is 3. |
| <b>Step 4</b> | Click <b>Save</b> .                                                                                            |
- 

### Configure SSO Mode on the Cisco EPN Manager Server

The SSO functionality distributes CA and self-signed certificate when the SSO server is added to the SSO client.

Cisco EPN Manager supports CA and self-signed certificates as long as the Common Name (CN) field of the certificate contains the Fully Qualified Domain Name (FQDN) of the server on both the SSO client and the SSO server. The server must be capable of name resolution from the IP address to the FQDN. In addition, the hostname must match the left-most component of the FQDN. SSO requires accurate DNS configuration. You must define the DNS with fully qualified domain name (FQDN). For example, the nslookup command and expected data when configuring DNS with FQDN is:

```
hostname CUSTOMER_HOSTNAME
nslookup CUSTOMER_HOSTNAME
Server:...
Address:...
Name: CUSTOMER_HOSTNAME.example.com
Address:....
```

For SSO operation, Cisco EPN Manager requires that the SSL/TLS certificate hold the FQDN in the CN field. To verify that the certificate used by your Cisco EPN Manager server has the FQDN in the CN field, use your browser to view the certificate. If the certificate does not contain the FQDN in the CN field, you must regenerate the certificate and redistribute it to all users that have the old certificate.



---

**Note** If you are using this procedure to configure SSO but are using local authentication, choose **Local** in Step 2.

---


- 
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **SSO Server Settings**.
- Step 2** Choose which SSO Server AAA Mode you want to use. You can select only one at a time.
- Step 3** Click **OK**.
-



## CHAPTER 26

# Fault Management Administration Tasks



**Note** Advanced users can also use the Cisco EPN Manager Representational State Transfer (REST) API to access device fault information. For information on the API, click  at the top right of the Cisco EPN Manager window, then choose **Help > API Help**.

- [Event Receiving, Forwarding, and Notifications, on page 705](#)
- [Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms, on page 708](#)
- [Change Event Severity Levels, on page 709](#)
- [Customize the Troubleshooting Text for an Alarm, on page 710](#)
- [Change Alarm Auto-Clear Intervals, on page 710](#)
- [Change the Information Displayed in the Failure Source for Alarms, on page 711](#)
- [Change the Behavior of Expedited Events, on page 711](#)
- [Customize Generic Events That Are Displayed in the Web GUI, on page 712](#)
- [Troubleshoot Fault Processing Errors, on page 713](#)
- [Get Help from the Cisco Support Community and Technical Assistance Center \(TAC\), on page 714](#)

## Event Receiving, Forwarding, and Notifications

Cisco EPN Manager processes syslogs and SNMPv1, v2, and v3 traps that it receives from devices. The server automatically listens for these events on UDP port 162. You do not have to perform any event listening configuration on the server, but you do have to configure devices to forward traps and syslogs to Cisco EPN Manager on the appropriate port.

Notifications are forwarded in SNMPv2 or SNMPv3 format. They are also forwarded to email recipients when you setup corresponding Notification Policies. If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is configured. Only INFO level events are processed for the selected category and alarms are processed with critical, major, minor and warning levels.

Cisco EPN Manager can forward alarms and events that are generated by the processing of received syslogs, traps, and TL/1 alarms to northbound notification receiver. Alarms of any severity can be forwarded, but only events with INFO severity can be forwarded. Information can be forwarded in :

- E-Mail format. See [Configure Default Settings for E-Mail Notifications, on page 707](#)

- SNMP trap format. See [Forward Alarms and Events as SNMP Trap Notifications, on page 707](#)

You can also use the SNMP trap notification mechanism to forward SNMP traps that indicate server problems. Alerts and events are sent as SNMPv2.

## Forward Alarms and Events as Email Notifications (Administrator Procedure)

When you configure an e-mail notification, e-mail is sent to the configured receivers when an alarm matching the criteria is created or updated. By default, the subject line includes the alarm severity and category. These settings, along with the message mode, are controlled from the system settings page for alarms and events. For more information, see [Configure Default Settings for E-Mail Notifications, on page 707](#).

If you want to forward generic (unsupported) events, make sure generic event handling is enabled. (To check the setting, see [Disable and Enable Generic Trap and Syslog Handling, on page 712](#).)

You can also forward alarms and events as SNMP trap notifications. For more information, see [Forward Alarms and Events as SNMP Trap Notifications, on page 707](#).

Users can also configure email notifications from the Alarms and Events page. Users are allowed to pick the event and severity, and specific a receiver's email address.

### Before you begin

If you have not configured the mail server, perform the instructions in [Set Up the SMTP E-Mail Server, on page 645](#). Otherwise notifications will not be sent.

- Step 1** Choose **Administration > Settings > System Settings**, then choose **Mail and Notification > Mail Server Configuration**.
- Step 2** In the **Sender and Receivers** area, add the receivers. You can specify multiple recipients as a comma-separated list.

| To forward alarms from specific categories to: | Do the following :                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The same receivers                             | <ol style="list-style-type: none"> <li>1. Enter the receiver(s) in the <b>To</b> field. Specify multiple receivers in a comma-separated list.</li> <li>2. Click the <b>Configure email notification for individual alarm categories</b> hyperlink and specify the data for the notification: <ul style="list-style-type: none"> <li>• Choose the alarms you want to include.</li> </ul> <p><b>Note</b> If you are forwarding server internal SNMP traps, choose the <b>System</b> category.</p> <ul style="list-style-type: none"> <li>• To specify alarms of specific severities, click the alarm name hyperlink, then choose the severities.</li> </ul> <p><b>Note</b> Do <i>not</i> enter any receiver e-mail addresses when you specific the alarm severities.</p> </li> <li>3. Click <b>Save</b> to save the alarm categories and their settings.</li> </ol> |



|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To different receivers | <ol style="list-style-type: none"> <li>1. Do <i>not</i> enter any e-mail addresses in the <b>To</b> field.</li> <li>2. Click the <b>Configure email notification for individual alarm categories</b> hyperlink.<br/><b>Note</b> If you are forwarding server internal SNMP traps, choose the <b>System</b> category.</li> <li>3. Select the alarms in which you are interested. You can specify the severities by clicking the alarm link and choosing <b>Critical</b>, <b>Major</b>, <b>Minor</b>, or <b>Warning</b>.<br/><b>Note</b> If you are forwarding server internal SNMP traps, choose the <b>System</b> category.</li> <li>4. Click <b>Save</b> to save the alarm categories and their settings.</li> </ol> |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Step 3** Click **Test**, to send a test email using the parameters you configured. The results of the test operation appear on the same page. The test feature checks connectivity to both primary and secondary mail servers by sending an email with a "Cisco EPN Manager test email" subject line.

**Step 4** Click **Save** to save the new notifications.

## Configure Default Settings for E-Mail Notifications

If you have not configured the mail server, perform the instructions in [Set Up the SMTP E-Mail Server, on page 645](#). Otherwise notifications will not be sent.

You can configure certain default settings that are applied across all alarm and event e-mail notifications. These settings can be overwritten when users configure individual notifications and receivers.

By default, the email subject line will include the alarm severity and category. The following settings are also available but are disabled by default.

- Subject line—Include the prior alarm severity or add custom text. Alternatively you can replace all of the subject line with custom text.
- Body of the email—Include custom text, the alarm condition, and a link to the alarm detail page.
- Secure message mode—Enabling this mode masks the IP address and controller name.

To enable, disable, or adjust these settings, choose **Administration > Settings > System Settings**, then **Alarms and Events > Alarms and Events**. Make your changes in the **Alarm Email Options** area.

For information on configuring an e-mail notification, see [Forward Alarms and Events as Email Notifications \(Administrator Procedure\), on page 706](#).

## Forward Alarms and Events as SNMP Trap Notifications

Cisco EPN Manager can forward alarms and events in EPM-NOTIFICATION-MIB format as an SNMPv2c and SNMPv3 trap notifications. You can specify:

- A specific alarm or event category, such as **System** for internal server SNMP traps.
- Alarms of a specific severity. Only INFO *events* are forwarded; you cannot specify other severities for events.

Before a notification is sent, Cisco EPN Manager pings the receiver to ensure it can be reached. If it does not respond, an alarm is generated to notify that the device is unreachable.



**Note** Cisco EPN Manager sends traps to notification receivers on port 162.

You can also forward alarms and events as email notifications. For more information, see [Forward Alarms and Events as Email Notifications \(Administrator Procedure\)](#), on page 706.

- 
- Step 1** As a user with Admin privileges, choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Notification Receivers**.
- Step 2** Select **Add Notification Receiver** from the **Select a command** drop-down list, then click **Go**.
- Step 3** Configure the new notification receiver.
- Provide the IP address and server name.
    - **IP Address**—Enter the IPv4 or IPv6 address of the server on which the receiver will run.
    - **Server Name**—Enter the host name of the server on which the receiver will run.
  - Click the **North Bound** radio button. The notification type defaults to UDP.
  - Enter the port number and SNMP version. The receiver that you configure should be listening to UDP on the same port that is configured.
 

**Note** Do not change the port number.

    - For SNMPv2c, enter the community string.
    - For SNMPv3, enter the username and password (the Engine ID is auto-populated), then select a mode from the Mode drop-down list (depending on the security level).
- Step 4** Specify the category and (for alarms) severity of the alarms and events you want to forward.
- Note** Generic events will only be forwarded if generic event handling is enabled. To check the setting, see [Disable and Enable Generic Trap and Syslog Handling](#), on page 712.
- Under **Category**, check all alarm types to be forwarded. If you are forwarding server internal SNMP traps, choose **System**.
  - Under **Severity**, select the highest Severity Level that you set when you configured the trap notifications themselves.
- Step 5** When you are finished, click **Save**.
- 

## Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms

The following table lists some display options for acknowledged, cleared, and assigned alarms. These settings *cannot* be adjusted by individual users (in their display preferences) because, for very large systems, a user could make a change that will impact system performance.

Other settings shown on the Alarms and Events page can be adjusted by users, but you can set the global defaults here. For information on those settings, see these topics:

- [Configure Default Settings for E-Mail Notifications, on page 707](#)
- [Alarm, Event, and Syslog Purging, on page 664](#)

**Step 1** Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarms and Events**.

**Step 2** Under the Alarm Display Options area, enable or disable these settings, as desired:

| Alarm Display Options                       | Description                                                                                                                                              | Does setting also affect search results? |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <b>Hide acknowledged alarms</b>             | Do not display Acknowledged alarms in the Alarms list or include them in search results                                                                  | Yes                                      |
| <b>Hide assigned alarms</b>                 | Do not display assigned alarms in the Alarms list or in search results                                                                                   | Yes                                      |
| <b>Hide cleared alarms in alarm browser</b> | Do not display cleared alarms in the Alarms list or in search results<br><b>Note</b> Cleared alarms remain viewable under the <b>Cleared Alarms</b> tab. | No                                       |
| <b>Add device name to alarm messages</b>    | Include device name in e-mail notifications                                                                                                              | No                                       |

**Step 3** To apply your changes, click **Save** at the bottom of the Alarms and Events window.

## Change Event Severity Levels

Each alarm in Cisco EPN Manager has a severity. The alarm severity is determined by the most severe event associated to the alarm. You can adjust the severity for alarms by changing the severity for newly-generated events.



**Note** For alarms that are related to Cisco EPN Manager system administration, such as high availability, refer to [Customize Server Internal SNMP Traps and Forward the Traps, on page 652](#).

You can change the severity level for network- and device-level alarms in two ways:

- Threshold-crossing alarms generated by optical, Carrier Ethernet, device health, or interface health monitoring policies—Change the settings in the relevant monitoring policy. See [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 205](#).
- Specific alarms—Use the procedure in this section.

**Step 1** Choose **Administration > System Settings**, then choose **Alarms and Events > Alarm Severity and Auto Clear**.

- Step 2** Expand the categories available under the **Event Types** column, or search for the event type you want by entering all or part of the event text in the **Event Types** search field just below the column heading.
- Step 3** Select the events and set their new severity.
1. Check the event's check box.
  2. Choose a severity level from the **Severity** drop-down list or , then click **Save**.

## Customize the Troubleshooting Text for an Alarm

You can associate troubleshooting and explanatory information with an alarm so that users with access to the Alarms and Events tables will be able to see it. Use this procedure to add or change the information that is displayed in the popup window.

- Step 1** Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarm Severity and Auto Clear**.
- Step 2** Select an alarm, then click **Recommended Action**.
- Step 3** Add or change the content in the **Explanation** and **Recommended Actions** fields, then click **Save**. To revert to the default text, click **Reset** and **Save**.

## Change Alarm Auto-Clear Intervals

You can configure an alarm to auto-clear after a specific period of time. This is helpful in cases, for example, where there is no clearing event. Auto-clearing an alarm will not change the severity of the alarm's correlated events.

- Step 1** Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarm Severity and Auto Clear**.
- Step 2** Expand the categories available under the **Event Types** column, or search for the event type you want by entering all or part of the event text in the **Event Types** search field just below the column heading.
- Step 3** To change the auto-clear duration for an event or group of events:
- For a single event, check the event's check box, click in the **Auto Clear Duration** field, enter the new duration, then click **Save**.
  - For multiple events, select the events, then click **Alarm Auto Clear**, enter the new duration in the dialog box, then click **OK**.
- Step 4** Change the Auto Clear Interval by performing one of the following tasks:
- Click on the **Auto Clear Duration** field, enter the new interval, and click **Save**.
  - Select the check box of the event type, click **Alarm Auto Clear**, enter the new interval, and click **OK**.

# Change the Information Displayed in the Failure Source for Alarms

When an alarm is generated, it includes information about the source of the failure. Information is presented using a specific format. For example, performance failures use the format *MACAddress:SlotID*. Failure sources for other alarms may include the host name, IP address, or other properties. Adjust the properties and separators (a colon, dash, or number sign) that are displayed in the alarm's failure source using the following procedure.

- 
- Step 1** Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarms and Events**.
- Step 2** In the Failure Source Pattern area, select the alarm category you want to customize.
- Step 3** Adjust the failure source format as follows:
- To customize the *properties* that are displayed, click **Edit**, select the properties, then click **OK**. If a property is greyed-out, you cannot remove it.
  - To customize the *separators* that are displayed between the properties, click **Edit Separator**.
- Step 4** To apply your changes, click **Save** at the bottom of the Alarms and Events settings window.
- 

## Change the Behavior of Expedited Events

By default, when Cisco EPN Manager receives a configuration change event from a device, it waits 10 minutes before starting inventory collection in case other related events are sent. This prevents multiple collection processes from running at the same time. This is called the *inventory collection hold off time* and is set to 10 minutes by default. This setting is controlled from the Inventory system settings page (**Administration > Settings > System Settings > Inventory**).

Expedited events are handled differently. Although they use the same hold off time mechanism, expedited events use the value set in a rules file rather than the value set in the web GUI. The rules file also instructs Cisco EPN Manager whether to perform an inventory collection only on specific parts of the network element, or on the whole NE.

Cisco EPN Manager has multiple rules file that are stored in `/opt/CSColumos/conf/fault/correlationEngine`. Expedited event settings are controlled by the files that end in the string **EventBasedInventoryRules.xml**.

You can make the following changes to expedited events by editing a rules file.

- Adjust the hold off timer for a specific event by changing the following setting in the rules file:

```
<property name="holdoffTime" value="mins">
```

*mins* indicates the number of minutes Cisco EPN Manager should wait before performing any other actions in response to the even. The value of *mins* must be set to a minimum of 1 (minute).

- Reconfigure an event to be normal, rather than expedited, by removing the event from the rules file.

You do not have to restart Cisco EPN Manager after editing the rules file. The change takes effect from when you save the rules file.

# Customize Generic Events That Are Displayed in the Web GUI

You can customize the description and severity for generic events generated by SNMP traps and syslogs. Your customization will be displayed in the Events tab for SNMP trap events. If a MIB module is not loaded, you can load it manually and then customize the notifications provided in that MIB.

See [Customize Generic Events Based on SNMP Traps, on page 713](#), for information on how to customize these generic events.

## Disable and Enable Generic Trap and Syslog Handling

By default Cisco EPN Manager does not drop any received syslogs or traps. As mentioned in [How are Alarms and Events Created and Updated?, on page 214](#), Cisco EPN Manager maintains an event catalog that determines whether Cisco EPN Manager should create a new event for incoming syslogs or traps (and if it creates a new event, whether it should also create an alarm). If Cisco EPN Manager does not create an event, the trap or syslog is considered a *generic event*.

By default, Cisco EPN Manager does the following:

- Displays the generic events in the Events list.
- Forwards generic events in e-mail or SNMP trap notifications, after normalizing them using the CISCO-EPM-NOTIFICATION-MIB.

All of these events are assigned the MINOR severity, regardless of the trap contents, and fall under the alarm category Generic.

## Disable and Enable Generic Trap Processing

Use the genericTrap.sh command to manage generic syslogs.

To do the following:	Use this command:
Turn off generic trap processing	<code>/opt/CSCOlumos/bin/genericTrap.sh -l</code>
Turn on generic trap processing	<code>/opt/CSCOlumos/bin/genericTrap.sh -u</code>

## Disable and Enable Generic Syslog Processing

Use the genericSyslog.sh command to manage generic syslogs.

To do the following:	Use this command:
Turn off generic syslog processing	<code>/opt/CSCOlumos/bin/genericSyslog.sh -l</code>
Turn on generic syslog processing	<code>/opt/CSCOlumos/bin/genericSyslog.sh -u</code>

## Customize Generic Events Based on SNMP Traps

Cisco EPN Manager supports the customized representation of generic events in the GUI. Managed objects normally generate SNMP traps and notifications that contain an SNMP trap object identifier (SnmptTrapOID) and a variable bind object identifier (VarBindOIDs) in numerical format. Cisco EPN Manager translates the numeric SnmptTrapOIDs and VarBindOIDs into meaningful names using customized MIB modules, then displays the generic events in the web GUI (in the event tables, Device 360 view, and so forth). For more details on Generic Events see [How are Alarms and Events Created and Updated?](#), on page 214.

Using the SNMP MIB files that are packaged with Cisco EPN Manager, you can customize the defined MIBs for your deployment's technology requirement.

The following table illustrates how ObjectIDs are decoded and displayed in the GUI.

**Table 47: Example: ObjectID Representation**

OIDs before Decoding	OIDs after Decoding
snmptTrapOID = 1.3.6.1.4.1.9.10.120.0.1', Values: 1.3.6.1.4.1.9.10.119.1.1.2.1.11.7.1=1	mplsL3VpnVrfDown, values: mplsL3VpnVrfOperStatus.("vrf1").(1) = 1

Follow the steps below to create customized generic events.

- 
- Step 1** Select **Monitor > Monitoring Tools > Alarms and Events**.
  - Step 2** Click the **Events** tab.
  - Step 3** Click **Custom Trap Events** and then click **Upload New Mibs**.
  - Step 4** In the **Upload Mib** window, click **Upload New MIB** to upload a MIB file.
  - Step 5** If you upload a new MIB file, wait until the file upload is complete, and then click **Refresh MIBs** to have the newly added MIB included in the **MIB** drop-down list.
  - Step 6** Click **OK**.  
Cisco EPN Manager creates a new event type and alarm condition for the specified trap.
- 

## Troubleshoot Fault Processing Errors

If your deployment is having fault processing problems, follow this procedure to check the fault logs.

- 
- Step 1** Log in to Cisco EPN Manager with a user ID that has Administrator privileges.
  - Step 2** Select **Administration > Settings > Logging**, then choose **General Logging Options**.
  - Step 3** In the **Download Log File** area, click **Download**.
  - Step 4** Compare the activity recorded in these log files with the activity you are seeing in your management application:
    - console.log
    - ncs-x-x.log
    - decap.core.java.log

xmp\_correlation.log  
decap.processor.log

### What to do next

You can also get help from the Cisco support community. If you do need to open a support case, attach the suspect log files with your case. See [Get Help from the Cisco Support Community and Technical Assistance Center \(TAC\)](#), on page 714.

## Get Help from the Cisco Support Community and Technical Assistance Center (TAC)

- [Open a Cisco Support Case](#), on page 714
- [Join the Cisco Support Community](#), on page 715

## Open a Cisco Support Case

When you open a support case from the web GUI, Cisco EPN Manager automatically populates the case form with information it can retrieve from a device. This includes technical details about the device, configuration changes on the device, and all device events that occurred in the last 24 hours. You can also attach your own files to the case.

### Before you begin

You can open a support case from the web GUI if:

- Your administrator has configured Cisco EPN Manager to allow you to do so. See [Set Up Defaults for Cisco Support Requests](#), on page 654.
- The Cisco EPN Manager server has a direct connection to the internet, or a connection by way of a proxy server.
- You have a Cisco.com username and password.

**Step 1** Choose one of the following:

- From **Monitor > Monitoring Tools > Alarms and Events**. Click a single alarm, then choose **Troubleshoot > Support Case**. If you do not see the **Troubleshoot** button, widen your browser window.
- From the Device 360 view. Hover your mouse over a device IP address, then click the information icon. Choose **Support Request** from the **Actions** drop-down menu.

**Step 2** Enter your Cisco.com username and password.

**Step 3** Click **Create**. Cisco EPN Manager populates the form with data it retrieves from the device.

**Step 4** (Optional) Enter a Tracking Number that corresponds to your own organization's trouble ticket system.

**Step 5** Click **Next** and enter a description of the problem.



Cisco EPN Manager populates the form with data it retrieves from the device and automatically generates the necessary supporting documents.

If desired, upload files from your local machine.

**Step 6** Click **Create Service Request**.

---

## Join the Cisco Support Community

You can access and participate in discussion forums in the online Cisco Support Community. You will need a Cisco.com username and password.

---

**Step 1** Choose one of the following:

- From **Monitor > Monitoring Tools > Alarms and Events**. Click a single alarm, then choose **Troubleshoot > Support Forum**. If you do not see the **Troubleshoot** button, widen your browser window.
- From the Device 360 view. Hover your mouse over a device IP address, then click the information icon. Choose **Support Community** from the **Actions** drop-down menu.

**Step 2** In the Cisco Support Community Forum page, enter your search parameters to find what you need.

---





## CHAPTER 27

# Audits and Logs

- [Audit Configuration Archive and Software Management Changes \(Network Audit\)](#) , on page 717
- [Audit Changes Made By Users \(Change Audit\)](#), on page 717
- [Audit Actions Executed from the GUI \(System Audit\)](#), on page 719
- [System Logs](#), on page 719

## Audit Configuration Archive and Software Management Changes (Network Audit)

The **Network Audit** window displays changes made to devices using the Configuration Archive and Software Management features. To view these changes, choose **Inventory > Device Management > Network Audit**. Cisco EPN Manager lists the most recent devices changes including the type of change (Configuration Archive, Software Image Management). For examples, see:

- [Check the Network Audit for Configuration Archive Operations](#), on page 105
- [Check the Network Audit for Software Image Operations](#), on page 131

You can also view the most recent changes for a device in the **Recent Changes** tab of its Device 360 view. See [Get Basic Device Information: Device 360 View](#), on page 63.

## Audit Changes Made By Users (Change Audit)

Cisco EPN Manager supports managing change audit data in the following ways:

- [Generate a Change Audit Report](#), on page 717
- [Enable Change Audit Notifications and Configure Syslog Receivers](#), on page 718

## Generate a Change Audit Report

The Change Audit report lists the actions that users have performed using the Cisco EPN Manager features. The following table provides examples of what may appear in a Change Audit report.

Feature	Examples
Device management	Device '209.165.202.159' Added

Feature	Examples
User management	User 'mmjones' added
Administration	Logout successful for user jlsmith from 209.165.202.129 Authentication Failed. Login failed for user fjclark from 209.165.202.125
Configuration changes	CLI Commands : ip access-list standard testremark test
Monitoring policies	Monitoring Template 'IF Outbound Errors (Threshold)' Created
Configuration templates	Configuration Template 'Add-Host-Name-IOS-Test' Created
Jobs	'Show-Users-On-Device-IOS_1' job of type Config Deploy - Deploy View scheduled.
Inventory	Logical File '/bootflash/tracelogs/inst_cleanup_R0-0.log.19999.20150126210302' deleted.

You can schedule a Change Audit report to run on a regular basis and, if desired, Cisco EPN Manager can e-mail the results to you. You can also forward this information in a Change Audit notification (see [Enable Change Audit Notifications and Configure Syslog Receivers, on page 718](#)).

- 
- Step 1** Choose **Reports > Report Launch Pad**, then choose **Compliance > Change Audit**.
- Step 2** Click **New** to configure a new report.
- Step 3** In the **Settings** area, enter the report criteria (time frame, when to start the report, and so forth).
- Step 4** If you want to schedule the report to run at a later time, enter your settings in the **Schedule** area. You can also specify an e-mail address that the report should be sent to.
- Step 5** If you want to run the report immediately, click **Run** at the bottom of the window.
- The **Report Run Result** lists all users and the changes they made during the specified time period.
- 

## Enable Change Audit Notifications and Configure Syslog Receivers

If desired, you can configure Cisco EPN Manager to send a change audit notification when changes are made to the system. These changes include device inventory and configuration changes, configuration template and monitoring template operations, and user operations such as logins and logouts and user account changes.

You can configure Cisco EPN Manager to:

- Forward changes as change audit notifications to a Java Message Server (JMS).
- Send these messages to specific syslog receivers.

If you configure syslog receivers but do not receive syslogs, you may need to change the anti-virus or firewall settings on the destination syslog receiver to permit reception of syslog messages.

- 
- Step 1** Select **Administration > Settings > System Settings**, then choose **Mail and Notification > Change Audit Notification**.

**Step 2** Select the **Enable Change Audit Notification** check box to enable notifications.

**Step 3** If you want to send the messages to specific syslog receivers:

- a) Click the **Add** button (+) to specify a syslog receiver.
- b) In the **Syslog Receivers** area, enter the IP address, protocol, and port number of the syslog receiver.

You can repeat these steps as needed to specify additional syslog receivers.

**Step 4** Click **Save**.

**Note** It is recommended to restart the Cisco EPN Manager server for the records to be reflected in secure tls log.

## Audit Actions Executed from the GUI (System Audit)



**Note** Cisco EPN Manager sends all change audit notifications in XML format to the topic **ChangeAudit.All**. You must be subscribed to **ChangeAudit.All** to receive the notifications.

The System Audit window lists all Cisco EPN Manager GUI pages that users have accessed. To view a System Audit, choose **Administration > Settings > System Audit**.

The following table shows some of the information you can find from the System Audit page using the quick filter. To enable the quick filter, choose **Quick Filter** from the **Show** drop-down list.

Find actions performed:	Do the following:
By a specific user	Enter the username in the <b>Username</b> quick filter field
By all users in a user group	Enter the group name in the <b>User Group</b> quick filter field
On devices in a specific virtual domain	Enter the virtual domain name in the <b>Active Virtual Domain</b> quick filter field
By the web GUI root user	Select <b>Root User Logs</b> from the <b>Show</b> drop-down list
On a specific device	Enter the IP address in the <b>IP Address</b> quick filter field
On a specific day	Enter the day in the <b>Audit Time</b> quick filter field (in the format <i>yyyy-mm-dd</i> )

## System Logs

Cisco EPN Manager provides three classes of logs which are controlled by choosing **Administration > Settings > Logging**.

Logging Type	Description	See:
<b>General</b>	Captures information about actions in the system.	<a href="#">View and Manage General System Logs, on page 720</a>
<b>SNMP</b>	Captures interactions with managed devices.	<a href="#">Enable SNMP Traces and Adjust SNMP Log Settings (Levels, Size), on page 721</a>
<b>Syslog</b>	Forwards Cisco EPN Manager audit logs (as syslogs) to another recipient.	<a href="#">Forward System Audit Logs As Syslogs, on page 721</a>

## View and Manage General System Logs

You can view system logs after downloading them to your local server.

- [View the Logs for a Specific Job, on page 720](#)
- [Adjust General Log File Settings and Default Sizes, on page 720](#)
- [Download and E-Mail Log Files for Troubleshooting Purposes, on page 721](#)
- [Forward System Audit Logs As Syslogs, on page 721](#)

### View the Logs for a Specific Job

- 
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
- Step 2** Choose a job type from the Jobs pane, then select a job instance from the Jobs window.
- Step 3** At the top left of the Job instance window, locate the **Logs** field, then click **Download**.
- Step 4** Open or save the file as needed.
- 

### Adjust General Log File Settings and Default Sizes

By default, Cisco EPN Manager logs all error, informational, and trace messages generated by all managed devices. It also logs all SNMP messages and Syslogs that it receives. You can adjust these settings, changing logging levels for debugging purposes.

To do the following:	From Administration > System Settings > Logging:
Change the size of logs, number of logs saved, and log naming convention	Adjust the Log File Settings. <b>Note</b> Change these settings with caution to avoid impacting the system.
Change the logging level for specific modules	In the General Log Settings, select the files and the desired level, and click <b>Save</b> . You will have to restart Cisco EPN Manager for the changes to take effect.
Download log files for troubleshooting purposes	In the Download Log File area, click <b>Download</b> .

To do the following:	From Administration > System Settings > Logging:
E-mail log files (for example, to the Cisco Technical Center)	Enter a comma-separated list of e-mail IDs and click <b>Send</b> .

## Download and E-Mail Log Files for Troubleshooting Purposes



**Note** This procedure sets and log message levels to Trace. Be sure to return the log message levels to their original setting so system performance is not impacted.

- Step 1** Choose **Administration > Settings > Logging**, then choose **General Logging Options**.
- Step 2** Note the setting in the **Message Level** drop-down list because you will need to reset it later.
- Step 3** In the **Enable Log Modules** area, select the **Log Modules** check box to select all modules.
- Step 4** Select **Trace** from the **Message Level** drop-down list.
- Step 5** Reproduce the problem on the system so the details can be captured in the logs.
- Step 6** In the **Download Log File** area, click **Download**. The download zip file will have the name:  
NCS-hostname-logs-yy-mm-dd-hh-mm-ss.  
The file includes an HTML file that lists all files included in the zip file.
- Step 7** In the E-Mail Log File area, enter a comma-separated list of e-mail IDs.
- Step 8** Revert to the original setting in the **Message Level** drop-down list.

## Forward System Audit Logs As Syslogs

- Step 1** Choose **Administration > Settings > Logging**, then choose **Syslog Logging Options**.
- Step 2** Select the **Enable Syslog** check box to enable collecting and processing system logs.
- Step 3** In the **Syslog Host** field, enter the IP address of the interface from which the message is to be transmitted.
- Step 4** From the **Syslog Facility** drop-down list, choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.
- Step 5** Click **Save**.

## Enable SNMP Traces and Adjust SNMP Log Settings (Levels, Size)

Enable SNMP tracing to access more detailed information about the packets sent and received through SNMP. You may want to do this when troubleshooting, such as when a trap is dropped.

To make the following changes, choose **Administration > Settings > Logging**, then choose **SNMP Logging Options**.

If you want to:	Do the following:
Enable SNMP tracing on specific devices	<p>In the <b>SNMP Log Settings</b> area:</p> <ol style="list-style-type: none"><li>1. Select the <b>Enable SNMP Trace</b> check box and the <b>Display Values</b> check boxes.</li><li>2. Enter the IP addresses of the devices you want to trace and click <b>Save</b>.</li></ol>
Change the size of logs and number of logs saved	<p>In the <b>SNMP Log File Settings</b> area:</p> <p><b>Note</b> Be careful when you change these settings so that you do not impact system performance (by saving too much data).</p> <ol style="list-style-type: none"><li>1. Adjust the maximum number of files and file size.</li><li>2. Restart Cisco EPN Manager for your changes to take effect. See <a href="#">Stop and Restart Cisco EPN Manager</a>, on page 647.</li></ol>





## CHAPTER 28

# Configure High Availability

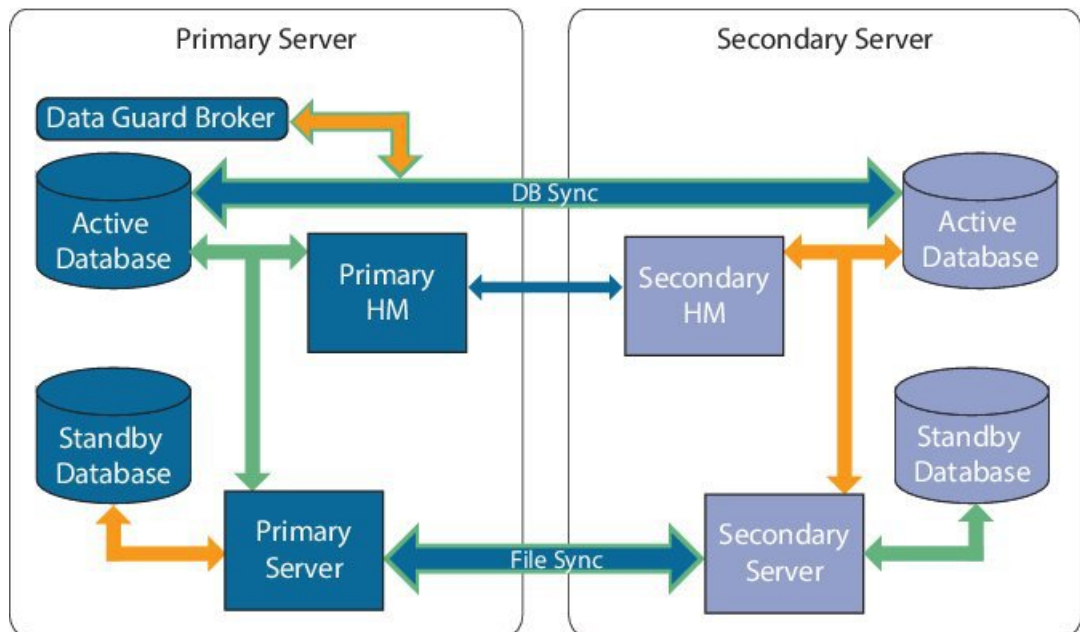
- [How High Availability Works, on page 723](#)
- [Set Up High Availability, on page 727](#)
- [Monitor HA Status and Events, on page 732](#)
- [Trigger Failover, on page 736](#)
- [Trigger Failback, on page 736](#)
- [Common Failover/Failback Scenarios, on page 737](#)
- [High Availability CLI Command Reference, on page 742](#)

## How High Availability Works

The Cisco EPN Manager high availability (HA) framework ensures continued system operation in case of failure. HA uses a pair of linked, synchronized Cisco EPN Manager servers to minimize or eliminate the impact of application or hardware failures that may take place on either server. Servers can fail due to issues in one or more of the following areas:

- Application processes—Server, TFTP, FTP, and other process failures. You can view the status of these processes using the CLI **ncs status** command.
- Database server—Database-related process failures (the database server runs as a service on Cisco EPN Manager).
- Network—Problems with network access or reachability.
- System—Problems with the server's physical hardware or operating system.
- Virtual machine (if HA is running in a VM environment)—Problems with the VM environment on which the primary and secondary servers are installed.

The following figure shows the main components and process flows for an HA setup.



An HA deployment consists of a primary and a secondary server with Health Monitor (HM) instances (running as an application process) on both servers. When the primary server fails (either automatically or because it is manually stopped), the secondary server takes over and manages the network while you restore access to the primary server. If the deployment is configured for automatic failover, the secondary server takes over the active role within two to three minutes after the failover. This HA is based on the *active/passive* or *cold standby* model of operation. Because it is not a clustered system, when the primary server fails, the sessions are not preserved in the secondary server.

When issues on the primary server are resolved and the server is in a running state, it remains in standby mode during which it begins syncing its data with the active secondary server. When the primary is available again, you can initiate a failback operation. When a failback is triggered, the primary server again takes over the active role. This role switching between the primary and secondary servers happens within two to three minutes.

Whenever the HA configuration determines that the primary server has changed, it synchronizes this change with the secondary server. These changes are of two types:

- File changes, which are synchronized using the HTTPS protocol. This includes items such as report configurations, configuration templates, TFTP-root directory, administration settings, licensing files, and the key store. File synchronization is done:
  - In batches, for files that are not updated frequently (such as license files). These files are synchronized once every 500 seconds.
  - Near real-time, for files that are updated frequently. These files are synchronized once every 11 seconds.
- Database changes, such as updates related to configuration, performance and monitoring data. Oracle Recovery Manager (RMAN) creates the initial standby database and Oracle Active Data Guard synchronizes the databases when there is any change.

The primary and secondary HA servers exchange the following messages to maintain synchronization between the two servers:

- Database Sync—Includes all the information necessary to ensure that the databases on the primary and secondary servers are running and synchronized.
- File Sync—Includes frequently updated configuration files. These are synchronized every 11 seconds, while other infrequently updated configuration files are synchronized every 500 seconds.
- Process Sync—Ensures that application- and database-related processes are running. These messages fall under the Heartbeat category.
- Health Monitor Sync—These messages check for the network, system, and health monitor failure conditions.

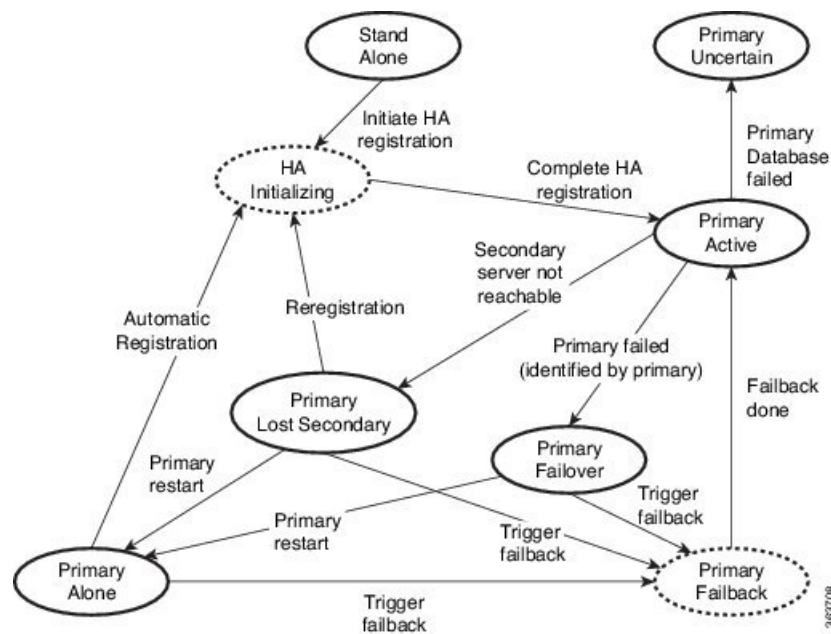
## HA States and Transitions

The following table lists the HA states, including those that require no response from you. You can view these states from the HA Status page (**Administration > Settings > High Availability > HA Status**) or from the Health Monitor. For a list of HA events and instructions for enabling, disabling, and adjusting them, see [Customize Server Internal SNMP Traps and Forward the Traps, on page 652](#).

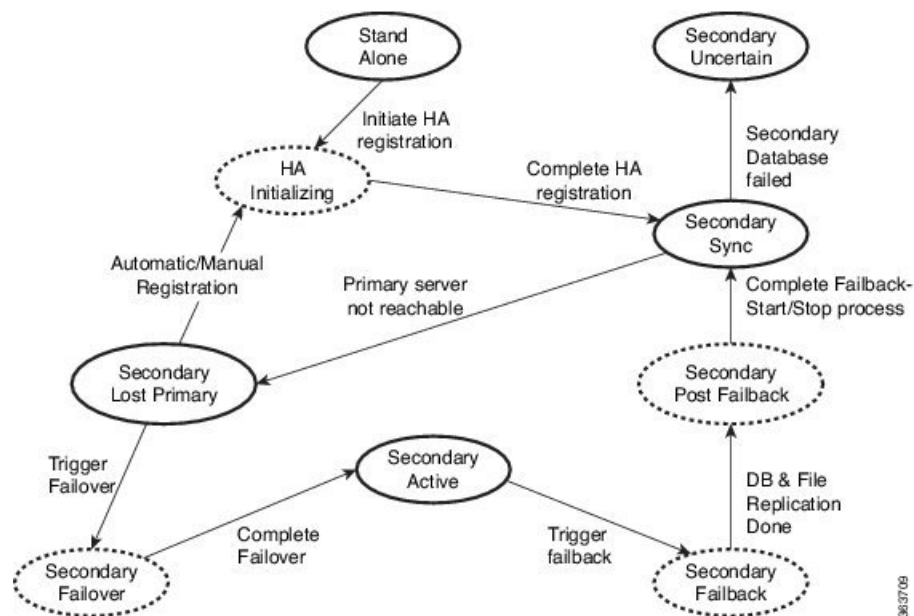
State	Server	Description
Stand Alone	Both	HA is not configured on this server.
Primary Alone	Primary	Primary server has restarted after it lost the secondary server (only Health Monitor is running in this state).
HA Initializing	Both	HA registration process between the primary and secondary server has started.
Primary Active	Primary	Primary server is now active and is synchronizing with the secondary server.
Primary Database Copy Failed	Primary	Restarted primary server detected a data gap, triggered a data copy from the active secondary server, and the database copy failed. When a primary server is restarted, it always checks to see if a data gap has occurred due to the primary server being down for 24 hours or more. This copy rarely fails but if it occurs, all attempts to failback to the primary are blocked until the database copy completes successfully. As soon as it does, the primary state is set to <b>Primary Syncing</b> .
Primary Failover	Primary	Primary server detected a failure.
Primary Failback	Primary	User-triggered failback is currently in progress.
Primary Lost Secondary	Primary	Primary server is unable to communicate with the secondary server.
Primary Preparing for Failback	Primary	Primary server has started up in standby mode after a failover (because the secondary server is still active). When the primary server is ready for failback, its state will be set to <b>Primary Syncing</b> .
Primary Syncing	Primary	Primary server is synchronizing the database and configuration files from the active secondary server. This occurs after a failover, when primary processes are brought up (and the secondary server is playing the active role).

Primary Uncertain	Primary	Primary server's application processes are not able to connect to its database.
Secondary Alone	Secondary	Primary server is not reachable from secondary server after a primary server restart.
Secondary Syncing	Secondary	Secondary server is synchronizing the database and configuration files from the primary server.
Secondary Active	Secondary	Failover from the primary server to the secondary server has completed successfully.
Secondary Lost Primary	Secondary	<p>Secondary server is not able to connect to the primary server (occurs when the primary fails or network connectivity is lost).</p> <p>For automatic failover, the secondary server will automatically move to the <b>Secondary Active</b> state. For Manual failover, you must trigger the failover to make the secondary server active (see <a href="#">Trigger Failover, on page 736</a>).</p>
Secondary Failover	Secondary	Failover triggered and is in progress.
Secondary Failback	Secondary	Failback triggered and database and file replication is in progress.
Secondary Post Failback	Secondary	Failback triggered; associated process stops and restarts are in progress. Database and configuration files have been replicated from the secondary server to the primary server. The primary server status will change to <b>Primary Active</b> , and the secondary server HA status will change to <b>Secondary Syncing</b> .
Secondary Uncertain	Secondary	Secondary server's application processes cannot connect to the server's database.

The following figure illustrates the primary server HA state changes.



This figure illustrates the secondary server HA state changes.



## Set Up High Availability

The [Cisco Evolved Programmable Network Manager Installation Guide](#) describes how to install the primary and secondary servers in your high availability deployment. As part of the installation, your administrator configures your HA deployment to use manual or automatic failover. You can check the current failover setting using the `ncs ha status` command or by checking the Health Monitor web page (see [Use the Health Monitor Web Page, on page 732](#)).

After the primary and secondary servers are installed, you must perform the HA registration steps described in [Register the Secondary Server for HA, on page 729](#).

The following topics describe additional setup tasks you may need to perform when managing your HA deployment.

- [Configure an SSO Server in an HA Environment, on page 731](#)
- [Reset the HA Authentication Key, on page 731](#)
- [Reset the Server IP Address or Host Name, on page 732](#)

## Using Virtual IP Addressing With HA

A virtual IP address represents the management IP address of the active HA server. During failover or failback, the virtual IP address automatically switches between the two HA servers. This provides two benefits:

- You do not need to know which server is active in order to connect to the Cisco EPN Manager web GUI. Using a virtual IP, your requests are automatically forwarded to the HA server that is active.
- You do not need to configure managed devices to forward notifications to both the primary server and the secondary server. Notifications only need to be forwarded to the virtual IP address.

Virtual IP addressing can be enabled when you register the secondary server with the primary server. You will need to provide the virtual address (IPv4 or IPv6) that you want both servers to share. See [Register the Secondary Server for HA, on page 729](#).

Using virtual IP addresses does not change the fact that active client-server sessions are terminated when a failover or failback occurs. Even though the virtual IP address will remain available, active client-server sessions (web GUI or NBI) are terminated as the new server begins servicing new requests. Web GUI users will have to log out and back in. For information on handling broken NBI sessions, see the [Cisco Evolved Programmable Network Manager MTOSI API Guide for OSS Integration](#).



---

**Note** To use a virtual IP, the IP addresses of the primary and secondary servers must be on the same subnet.

---

## What If I Cannot Use Virtual IP Addressing?

Depending on the deployment model you choose, not configuring a virtual IP address may result in the administrator having to perform additional steps in order to ensure that syslogs and SNMP notifications are forwarded to the secondary server in case of a failover. The usual method is to configure the devices to forward all syslogs and traps to both servers, usually via forwarding them to a given subnet or range of IP addresses that includes both the primary and secondary server.

This configuration work should be done at the same time HA is being set up: that is, after the secondary server is installed but before HA registration is done on the primary server. It must be completed before a failover so that the chance of losing data is eliminated or reduced. Not using a virtual IP address entails no change to the secondary server install procedure. The primary and secondary servers still need to be provisioned with their individual IP addresses, as normal.

## Register the Secondary Server for HA

These topics describe the HA registration process:

- [What Happens During Secondary Server Registration, on page 729](#)
- [Register the Secondary Server on the Primary Server, on page 729](#)
- [Troubleshoot an HA Registration Failure, on page 730](#)

### What Happens During Secondary Server Registration

After the secondary server is registered on the primary server, Cisco EPN Manager copies all database and configuration data from the primary to the secondary server. The length of this process depends on the amount of database and configuration data, as well as the available bandwidth on the network link between the two servers. The bigger the data and the slower the link, the longer the replication will take.

Cisco EPN Manager initiates synchronization between the primary and the secondary HA servers. The synchronization should not have any impact on user activity, although users may observe slow system response until the synchronization is complete. There is no impact on the execution of user- or system-related activity during the sync.

When Cisco EPN Manager is replicating the database, the secondary server itself will be in passive mode (and in the **Secondary Syncing** state), but all processes on the secondary server will be running. For example, if you execute the CLI command **ncs status** on the secondary server, the command output will show all processes as running.

### Register the Secondary Server on the Primary Server

After installing the secondary server, you must register it on the primary server. The registration steps must be performed from the primary server. (Installing the secondary server is described in the [Cisco Evolved Programmable Network Manager Installation Guide](#).)

#### Before You Begin

- Log in as the Linux CLI admin user, and stop and restart the primary and secondary servers by running the **ncs stop** and **ncs start** commands. Check that the services are up and running on both servers by running the **ncs status** command.
- If you are not using virtual IP addresses, make sure devices are configured to forward traps and syslogs to both the primary and secondary server. (For information on using virtual IP addresses with HA, see the [Cisco Evolved Programmable Network Manager Installation Guide](#). That guide explains any restrictions—for example, both servers must be on the same subnet to use virtual IP addresses.)



---

**Note**

If you choose to deploy the primary and secondary servers on the same IP subnet, you can configure your devices to send notifications to Cisco EPN Manager at a single virtual IP address. If you choose to disperse the two servers geographically, such as to facilitate disaster recovery, you will need to configure your devices to send notifications to both servers.

---

- Make sure you have the following information:
  - IP address or host name of the secondary server.
  - Password (authentication key) that was specified when installing the secondary server.



- An e-mail address for HA state change notifications.
- The preferred failover type (manual is recommended to avoid failovers that result from intermittent network outages).
- A web GUI user ID that has administrator privileges and access to ROOT-DOMAIN.

- 
- Step 1** On the primary server, log into the Cisco EPN Manager web GUI with a user ID that has administrator privileges.
- Step 2** Choose **Administration > Settings > High Availability**, then choose **HA Configuration**.
- Step 3** In the **General** area, complete the **Authentication Key**, **Email Address**, **Failover Type**, and **Secondary Server** fields. In the **Email Address** field, you can enter a comma-separated list of addresses to which notifications should be mailed. If you already configured email notifications, the email addresses you enter here will be appended to the list of addresses already configured (see [Forward Alarms and Events as Email Notifications \(Administrator Procedure\)](#), on page 706).
- Step 4** (If you are using the virtual IP feature) Check the **Virtual IP** check box, and then enter the virtual IPv4 or IPv6 address you want both servers to use.
- Step 5** Click **Save** to save your changes and initiate the HA registration process.
- Step 6** On the HA Configuration page, ensure that the **Configuration Mode** field displays the value **HA Enabled** to verify that the registration is successful. You can now log in to the Health Monitor.
- 

### What to do next

Monitor the server state changes that are listed in the following table. On the primary server's HA Status page, click **Refresh** to view the progress. (You can also view the status from either server using the Health Monitor web page.)

Server	Expected State Transitions
Primary	Stand Alone to HA Initializing to Primary Active
Secondary	Stand Alone to HA Initializing to Secondary Syncing

## Troubleshoot an HA Registration Failure

You can tell that registration has failed if the state of both the servers changes from **HA Initializing** to **Stand Alone**.

To recover from failed HA registration:

- 
- Step 1** Use ping and other tools to check the network connectivity between the two servers. Confirm that the secondary server is reachable from the primary server, and vice versa.
- Step 2** Check that the gateway, subnet mask, virtual IP address (if configured), server hostname, DNS, and NTP settings are all correct.
- Step 3** Check that configured DNS, NTP, and SSO servers are reachable from the primary and secondary servers, and that both are responding without latency or other network-specific issues.
- Step 4** Check that the required device and feature licenses are installed on the primary server.
-



**What to do next**

Once you have remedied any connectivity or setting issues, retry the steps in [Register the Secondary Server on the Primary Server, on page 729](#).

## Configure an SSO Server in an HA Environment

Single Sign-On (SSO) authentication is used to authenticate and manage users in a multi-user, multi-repository environment. SSO is responsible for storing and retrieving the credentials that are used for logging into different systems. You can set up a Cisco EPN Manager as the SSO server for other instances of Cisco EPN Manager.

To configure an SSO server in the high-availability environment, choose one of the procedures listed in the [Table 48: SSO Configuration in a HA Deployment](#). See these topics for more information:

- To configure the SSO server, see [Add a RADIUS or TACACS+ Server to Cisco EPN Manager, on page 691](#).
- To configure the HA servers, see the [Cisco Evolved Programmable Network Manager Installation Guide](#).

**Table 48: SSO Configuration in a HA Deployment**

SSO Configuration	Setup SSO Server	Sever Failover Scenario	SSO Server Failure Scenario
SSO as a standalone server	<ol style="list-style-type: none"> <li>1. Configure the standalone SSO server.</li> <li>2. Configure the primary and secondary HA servers.</li> </ol>	When the primary server fails, the secondary server is activated. All machines that are connected to the primary server will be redirected to the secondary server.	When the SSO server fails, SSO functionality is disabled. Cisco EPN Manager will use local authentication.
SSO on the secondary Server	<ol style="list-style-type: none"> <li>1. Configure one server to be the SSO server and the primary server (in other words, the primary server will also be the SSO server).</li> <li>2. Configure the secondary HA server.</li> </ol>	When the primary server fails, the secondary server is activated. All machines that are connected to primary server will not be redirected to the secondary server (because SSO is configured on the primary server).	When the SSO (primary) server fails, the secondary server can be set as the failback option for SSO. This enables all instances to connect to the secondary server.  If the secondary server is not set as the SSO server failback option, Cisco EPN Manager will use local authentication.

## Reset the HA Authentication Key

Users with administrator privileges can change the HA authentication key using the **ha authkey** command. You will need to ensure that the new authorization key meets the password standards.

- 
- Step 1** Log in to the primary server as a Cisco EPN Manager CLI admin user (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)).
- Step 2** Enter the following at the command line:

```
ha authkey newAuthKey
```

Where *newAuthKey* is the new authorization key.

---

## Reset the Server IP Address or Host Name

Avoid changing the IP address or hostname of the primary or secondary server, if possible. If you must change the IP address or hostname, remove the HA configuration from the primary server before making the change. When finished, re-register HA.

## Restore Data In an HA Deployment

Cisco EPN Manager does not back up configuration settings related to high availability. If you are restoring an implementation that is using HA, you should only restore data to the primary server. The restored primary server will automatically replicate its data to the secondary server. If you try to run a restore on a secondary server, Cisco EPN Manager will generate an error message.

Follow these steps when restoring an implementation that uses HA:

1. On the primary server, remove HA using the **ncs ha remove** command.
2. Restore data on the primary server, as described in [Restore Cisco EPN Manager Data, on page 626](#).
3. When the restore process is complete, perform the HA registration process again.

## Monitor HA Status and Events

These topics describe how to monitor the overall health of the HA environment:

- [Use the Health Monitor Web Page, on page 732](#)
- [HA Configuration Modes, on page 734](#)
- [HA States and Transitions, on page 725](#)
- [Check HA Status and Overall Health, on page 734](#)
- [View and Customize HA Events, on page 735](#)
- [Use HA Error Logging, on page 735](#)

## Use the Health Monitor Web Page

The Health Monitor is one of the main components that manage the HA operations. Health Monitor instances run on both servers as an application process, with its own web page on each server. It performs the following functions:

- Synchronizes database and configuration data related to HA (this excludes databases that synchronize separately using Oracle Data Guard).
- Exchanges heartbeat messages between the primary and secondary servers every 5 seconds, to ensure communications are maintained between the servers. If the healthy server does not receive 3 consecutive heartbeats from the other redundant server, it waits for 10 seconds. The healthy server then attempts to

open a web URL in the redundant server. If this attempt fails, the healthy server becomes the active server.

- Checks the available disk space on both servers at regular intervals and generates events when storage space runs low.
- Manages, controls, and monitors the overall health of the linked HA servers. If there is a failure on the primary server, the Health Monitor activates the secondary server.

After you have completed HA registration successfully, you can access the Health Monitor web page from the primary or secondary server by entering the following URL on your browser:

**https://ServerIP:8082**

where *ServerIP* is the primary or secondary server's IP address or host name.

The following example shows a Health Monitor web page for a secondary server in the **Secondary Active** state.

The screenshot shows the Cisco EPN Manager Health Monitor web page. The header includes the Cisco logo, the title "EPN Manager Health Monitor", and the server state "Secondary". Navigation links for "Software Update", "Refresh", and "Logout" are present. The main content area is divided into several sections:

- Health Monitor Details:** Shows the version as 3.0 (3.0.0.0.66).
- Settings:** A section for configuring the health monitor.
- Status:** Displays the current state as "Secondary Active" with a green checkmark icon. It also shows the "Primary IP Address" as 192.0.2.122, the "Failover Type" as "Manual", and an "Action" button labeled "Failback".
- Logging:** Includes a "Message Level" dropdown set to "Information" and a "Save" button.
- Download Health Monitor Log Files:** Includes a "Download" button.
- Events:** A table listing recent events in chronological order, with the most recent at the top.

Numbered annotations on the screenshot:

- Points to the "Settings" link.
- Points to the "Status" section.
- Points to the "Events" section.
- Points to the "Primary IP Address" field.
- Points to the "State" field.
- Points to the "Failover Type" field.
- Points to the "Action" button.
- Points to the "Message Level" dropdown.
- Points to the "Save" button.
- Points to the "Download" button.

1	Settings—Displays the Health Monitor state and configuration detail in five separate sections.	2	Status—Indicates the current functional status of the HA setup (a green check mark indicates HA is enabled and working).
3	Events—Displays the current HA-related events in chronological order, with the most recent events at the top.	4	Primary/Secondary IP address—Displays the IP address of the paired servers. Because this Health Monitor instance is running on the secondary server, it shows the IP address of the primary server.

5	Download—Lets you download the Health Monitor log files.	6	State—Shows the current state of the server on which this Health Monitor instance is running (in this case, the secondary server).
7	Message Level—Indicates the current logging level, which you can change (Error, Informational, or Trace). You must click <b>Save</b> to change the logging level.	8	Title bar—Identifies the HA server whose Health Monitor web page you are viewing, along with the Refresh and Logout buttons. Note that the Software Update is only displayed for secondary servers.
9	Failover Type—Shows whether you have Manual or Automatic failover configured.	10	Action—Shows the actions you can perform, such as failover or failback. Only the available actions are displayed here.

## HA Configuration Modes

HA configuration modes represent the overall status of the complete HA configuration (as opposed to HA states, which are specific to a server).

Mode	Description
HA Not Configured	HA is not configured on this server.
HA Initializing	HA registration process between the primary and secondary servers has started.
HA Enabled	HA is enabled between the primary and secondary servers.
HA Alone	Server is running alone because one of the servers is down, out of sync, or unreachable.

## Check HA Status and Overall Health

You can use the Cisco EPN Manager web GUI or CLI to check HA status. Either of these approaches will list the state of the server. States are described in [HA States and Transitions, on page 725](#).

To check the HA status from the web GUI, do one of the following:

- From the Cisco EPN Manager web GUI—Choose **Administration > Settings > High Availability**, then choose **HA Status**. The current HA status and the event states are displayed.
- From the Health Monitor. See [Use the Health Monitor Web Page, on page 732](#).

To check HA status from the CLI, log into either server as a CLI admin user (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)). The `ncs ha status` command provides a HA-specific output similar to the below example:

```
ncs ha status
[Role] Secondary [Primary Server] cisco-hal(192.0.2.133) [State] Secondary Active [Failover
Type] Manual
```

Use the `ncs status` command to check the Health Monitor and other server processes. You will see an output similar to the following example:

```
ncs status
Health Monitor Server is running. ( [Role] Secondary [State] Secondary Active )
Database server is running
Ftp Server is running
Tftp Server is running
Matlab Server is running
Matlab Server Instance 1 is running
Matlab Server Instance 2 is running
Matlab Server Instance 3 is running
NMS Server is running.
Plug and Play Gateway is running.
SAM Daemon is running ...
DA Daemon is running ...
```

## View and Customize HA Events

HA-related alarms are listed in the Alarms and Events table. A list of these alarms is provided in [Cisco Evolved Programmable Network Manager Supported Alarms](#). The following procedure explains how to view these alarms in the web GUI.

If desired, you can also:

- Adjust the severity for these alarms
- Configure notifications for these alarms

For more information, see [Work With Server Internal SNMP Traps That Indicate System Problems](#), on page 652.

To view HA-related alarms:

- 
- |               |                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Monitor &gt; Monitoring Tools &gt; Alarms and Events</b> , then click the <b>Alarms</b> tab. |
| <b>Step 2</b> | Choose <b>Quick Filter</b> from the <b>Show</b> drop-down list at the top right of the table.          |
| <b>Step 3</b> | In the <b>Message</b> field, enter <b>High Availability</b> .                                          |
- 

## Use HA Error Logging

To save disk space and maximize performance, HA error logging is disabled by default. If you are having trouble with HA, complete the following procedure to enable error logging and examine the log files.

- 
- |               |                                                                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Launch the Health Monitor on the server that is having trouble (see <a href="#">Use the Health Monitor Web Page</a> , on page 732).                                                                                                                             |
| <b>Step 2</b> | In the <b>Logging</b> area, select the error-logging level from the <b>Message Level</b> drop-down list and then click <b>Save</b> .                                                                                                                            |
| <b>Step 3</b> | Download the log files you want to examine: <ol style="list-style-type: none"><li>1. Click <b>Download</b>.<br/>A .zip file is copied to your default download location.</li><li>2. Extract the log files and use any ASCII text editor to view them.</li></ol> |
-

# Trigger Failover

Failover activates the secondary server in response to a failure detected on the primary server.

The Health Monitor detects failure conditions using the heartbeat messages exchanged between the two HA servers. The heartbeat messages are sent every 5 seconds, and if the primary server is not responsive to three consecutive heartbeat messages from the secondary server, the Health Monitor deems the primary server to have failed. During the health check, the Health Monitor also checks the application process status and database health. If there is no proper response to these checks, these are also treated as having failed.

The HA system in the secondary server takes about 15 seconds to detect a process failure on the primary server. If the secondary server is unable to reach the primary server due to a network issue, it might take more time to discover the failure and initiate a failover. In addition, it may take additional time for the application processes on the secondary server to be fully operational.

As soon as the Health Monitor detects a failure, it sends an e-mail notification. The e-mail includes the failure status along with a link to the secondary server's Health Monitor web page. If HA is configured for automatic failover, the secondary server will activate automatically.

To perform a manual failover:

## Before you begin

- Check the state of the primary and secondary servers.
- Validate the connectivity between the two servers.
- If you are not using virtual IP addresses, make sure all devices are configured to forward traps and syslogs to both servers.

---

**Step 1** Access the secondary server's Health Monitor web page using the web link given in the email notification, or by entering the following URL on your browser:

`https://ServerIP:8082`

**Step 2** Click **Failover**.

---

# Trigger Failback

Failback is the process of re-activating the primary server once it is back online. It also transfers Active status from the secondary server to the primary server, and stops active network monitoring processes on the secondary server.

When a failback is triggered, the secondary server replicates its current database information and updated files to the primary server. The time it takes to complete the failback from the secondary server to the primary server will depend on the amount of data that needs to be replicated and the available network bandwidth.

Once the data has begun replicating successfully, HA changes the state of the primary server to **Primary Active** and the state of the secondary server to **Secondary Syncing**.

During failback, the availability of the secondary server depends on whether the Cisco EPN Manager was reinstalled on the primary server after the failover, as follows:

- If Cisco EPN Manager was reinstalled on the primary server after the failover, a full database copy will be required and the secondary server will not be available during the failback process.
- If Cisco EPN Manager was not reinstalled with primary server, the secondary server is available, except during the period when processes are started on the primary server and stopped on the secondary server. Both servers' Health Monitor web pages are accessible for monitoring the progress of the failback. Additionally, users can also connect to the secondary server to access all normal functionalities.

You must always trigger failback manually, as described in the procedure below. Note:

- Do not initiate configuration or provisioning activity while the failback is in progress.
- After a successful failback, the secondary server will go down and control will switch over to the primary server. During this process, Cisco EPN Manager will be inaccessible to the users for a few moments.

#### Before you begin

- Check the state of the primary and secondary servers.
- Validate the connectivity between the two servers.
- If you are not using virtual IP addresses, make sure all devices are configured to forward traps and syslogs to both servers.
- If you have reinstalled Cisco EPN Manager on the primary server and you are using offline geo maps, you must reinstall the geo maps resources on the primary server before triggering failback. See the [Cisco Evolved Programmable Network Manager Installation Guide](#).

---

**Step 1** Access the secondary server's Health Monitor web page using the link given in the e-mail notification, or by entering the following URL on your browser:

`https://ServerIP:8082`

**Step 2** Click **Failback**.

---

## Common Failover/Failback Scenarios

The following topics describe common HA scenarios that may require failover and failback.

- [Network is Down, on page 738](#)
- [Process Restart Fails, on page 738](#)
- [Primary Server Restarts During Synchronization, on page 739](#)
- [Secondary Server Restarts During Synchronization, on page 739](#)
- [How to Recover From Split-Brain Scenario, on page 739](#)
- [Both HA Servers Are Powered Down, on page 739](#)
- [Both HA Servers Are Down and Secondary Server Will Not Restart, on page 740](#)
- [Replace the Primary HA Server, on page 741](#)
- [Secondary Server Goes Down, on page 741](#)

## Network is Down

If there is a loss of network connectivity between the primary and secondary servers, you will get e-mail notifications that each server has lost connectivity to the other server.

### If Automatic Failover is Configured:

After the failover is complete, you will receive an e-mail notification that the secondary server is now active.

1. Check for and restore network connectivity between the two servers.
2. Restart the primary server.
3. Trigger a failback from the secondary to the primary server (see [Trigger Failback, on page 736](#)).

### If Manual Failover is Configured:

1. Check for and restore network connectivity between the two servers.
2. Use the Health Monitor web page for the secondary server, to trigger a failover from the primary server to the secondary server (see [Use the Health Monitor Web Page, on page 732](#)).
3. Once you receive an e-mail notification that the secondary is now active, trigger a failback from the secondary server to the primary server (see [Trigger Failback, on page 736](#)).

## Process Restart Fails

The Cisco EPN Manager Health Monitor process is responsible for attempting to restart any Cisco EPN Manager server processes that have failed. The current state of the primary and secondary servers should be **Primary Active** and **Secondary Syncing** at the time any such failures occur.

If Health Monitor cannot restart a critical process on the primary server, then the primary server is considered to have failed. You will receive an email notification of this failure.

### If Automatic Failover is Configured:

After the failover is complete, you will receive an email notification that the secondary server is now active.

1. Restart the primary server and ensure that it is running. When the primary server is up, its HA state will be **Standalone**.
2. Trigger a failback from the secondary to the primary server (see [Trigger Failback, on page 736](#)).

### If Manual Failover is Configured:

1. Trigger a failover from the primary to the secondary (see [Trigger Failover, on page 736](#)).
2. Restart the primary server and ensure that it is running. When the primary server is up, its HA state will be **Standalone**.
3. Trigger a failback from the secondary to the primary (see [Trigger Failback, on page 736](#)).



## Primary Server Restarts During Synchronization

### If Manual Failover is Configured:

If the primary server is restarted while the secondary server is synchronizing, the **Standalone** and the **HA Initializing** states occur immediately after the primary comes back online. No administrator response should be required.

### If Automatic Failover is Configured:

If the primary server is restarted while the secondary server is synchronizing, you must trigger a failback from the secondary to the primary (see [Trigger Failback, on page 736](#)).

## Secondary Server Restarts During Synchronization

If the secondary server is restarted while syncing with the primary server, you will see the same state transitions regardless of the Failover Type settings. No administrator response should be required.

## How to Recover From Split-Brain Scenario

In a split-brain scenario, both the primary and secondary servers become active at the same time, perhaps due to a network outage or a link that temporarily goes down. However, because the primary server constantly checks the secondary server, when the connection is reestablished, the primary server will go down due to the secondary server being active.

The possibility of data loss always exists on the rare occasions when a “split-brain scenario” occurs. In this case, you can choose to save the newly added data on the secondary and forget the data that was added on the primary, as explained in the following steps.

- 
- |               |                                                                                                                                                                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Once the network is up, and the secondary server is up, the primary will restart itself automatically, using its standby database. The HA status of the primary server will be, first, “Primary Failover” transitioning to “Primary Syncing”. You can verify this by logging on to the primary server’s Health Monitor web page. |
| <b>Step 2</b> | Once the primary server’s status is “Primary Syncing, confirm that a user can log into the secondary server’s Cisco EPN Manager page using the web browser (for example, <a href="https://server-ip-address:443">https://server-ip-address:443</a> ). Do not proceed until you have verified this.                               |
| <b>Step 3</b> | Once access to the secondary is verified, initiate a failback from the secondary server's Health Monitor web page (see <a href="#">Trigger Failback, on page 736</a> ). You can continue to perform monitoring activities on the secondary server until the switchover to the primary is completed.                              |
- 

## Both HA Servers Are Powered Down

If both the primary and secondary servers are down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

## Both HA Servers Are Down and Secondary Server Will Not Restart

- 
- Step 1** Power on the secondary server and the Cisco EPN Manager instance running on it. The secondary HA restart will fail at this state because the primary server is not reachable. However, the secondary server's HM process will be running (with an error).
- Step 2** When Cisco EPN Manager is running on the secondary server, access the secondary server's HM web page (see [Use the Health Monitor Web Page, on page 732](#)). You will see the secondary server transition to the **Secondary Lost Primary** state.
- Step 3** Power on the primary server and the Cisco EPN Manager instance running on it.
- Step 4** When Cisco EPN Manager is running on the primary server, the primary server will automatically begin syncing with the secondary server. To verify this, access the primary server's HM web page. You will see the two servers transition through the following series of HA states:
- Primary server will change from **Primary Lost Secondary** to **Primary Active**.
  - Secondary server will change from **Secondary Lost Primary** to **Secondary Syncing**.
- Step 5** Restart the secondary server and the Cisco EPN Manager instance running on it. This is required because not all processes will be running on the secondary server at this point.
- If for some reason you cannot restart the secondary server, see [Both HA Servers Are Down and Secondary Server Will Not Restart, on page 740](#).
- Step 6** When Cisco EPN Manager finishes restarting on the secondary server, all processes should be running. Verify this by running the `ncs ha status` command.
- 

## Both HA Servers Are Down and Secondary Server Will Not Restart

If both HA servers are down at the same time and the secondary server will not restart, you will need to remove the HA configuration from the primary server in order to use it as a standalone server until you can replace or restore the secondary server.

- 
- Step 1** Attempt to restart the primary instance of Cisco EPN Manager. If the primary server is able to restart at all, the restart will abort with an error message indicating that you must remove the HA configuration.
- Step 2** Open a CLI session with the primary server (see [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#)).
- Step 3** Enter the following command to remove the HA configuration on the primary server:
- ```
ncs ha remove
```
- Step 4** Confirm that you want to remove the HA configuration.
- Step 5** Enter N (no) when you are prompted to confirm that you want to remove all of the HA database information from both the primary and secondary servers.
- You should now be able to restart the primary instance of Cisco EPN Manager without receiving an error message, and use it as a standalone server. When you are able to restore or replace the secondary server, proceed as explained in [Register the Secondary Server on the Primary Server, on page 729](#).
-

## Replace the Primary HA Server

Under normal circumstances, the state of your primary server will be **Primary Active** and your secondary server will be **Secondary Syncing**. If the primary server fails for any reason, a failover to the secondary will take place (automatically or manually).

You may find that restoring full HA access requires you to reinstall the primary server using new hardware. If this happens, you can follow the steps below to bring up the new primary server without losing any data.

### Before you begin

Make sure you have the password (authentication key) that was set when HA was configured on the secondary server. You will need it for this procedure.

- 
- Step 1** Ensure that the secondary server is in the **Secondary Active** state. If the primary server is configured for manual failover, you will need to trigger failover to the secondary server (see [Trigger Failover, on page 736](#)).
- Step 2** Ensure that the old primary server you are replacing has been disconnected from the network.
- Step 3** Ensure that the new primary server is ready for use. This will include connecting it to the network and configuring it similar to the old primary server (IP address, subnet mask, and so forth). You will need to enter the same authentication key that you entered when installing HA on the secondary server.
- Step 4** Trigger a failback from the secondary server to the newly-installed primary server. You will see the two servers transition through the following series of HA states:
- Primary server will transition from **HA Not Configured** to **Primary Failback** to **Primary Active**.
  - Secondary server will transition from **Secondary Active** to **Secondary Failback** to **Secondary Post Failback** to **Secondary Syncing**.
- 

## Secondary Server Goes Down

In this scenario, the secondary server is acting as a standby server and it goes down.

To get the secondary server up and running again:

- 
- Step 1** Power on the secondary server.
- Step 2** Start Cisco EPN Manager on the secondary server.
- Step 3** On the primary server, verify that the primary server's HA status changes from "Primary Lost Secondary" to "Primary Active." Go to **Administration > Settings > High Availability > HA Configuration**.
- Step 4** Log into the secondary server's Health Monitor page by entering the following URL in your browser:  
**https://serverIP:8082**.
- Step 5** Verify that the secondary server's HA status changes from "Secondary Lost Primary" to "Secondary Syncing." No further action is required once the above statuses are displayed. However, if the HA status does not change, the secondary server cannot be recovered automatically. In this case, continue with the following steps.
- Step 6** Remove the HA configuration on the primary server. Go to **Administration > Settings > High Availability > HA Configuration** and click **Remove**.
- Step 7** Register the secondary server with the primary server. See [Register the Secondary Server for HA, on page 729](#).

If HA registration is successful, no further action is required. However, if HA registration is unsuccessful, it indicates that the secondary server might have suffered hardware/software loss. In this case, continue with the following steps.

- Step 8** Remove the HA configuration on the primary server.
- Step 9** Reinstall the secondary server with the same release and patches (if any) as the primary server.
- Step 10** Register the secondary server with the primary server. See [Register the Secondary Server for HA, on page 729](#).
- 

## High Availability CLI Command Reference

The following table lists the CLI commands available for HA management. You must be logged in as the admin CLI user to use these commands. The output reflects the status of the server you are using. In other words, if you run **ncs ha status** from the primary server, Cisco EPN Manager reports the status of the primary server.

**Table 49: High Availability Commands**

| Command                                 | Description                                           |
|-----------------------------------------|-------------------------------------------------------|
| <b>ncs ha ?</b>                         | Displays the command usage message.                   |
| <b>ncs ha authkey <i>newAuthkey</i></b> | Updates the authentication key to <i>newAuthKey</i> . |
| <b>ncs ha remove</b>                    | Removes the HA configuration.                         |
| <b>ncs ha status</b>                    | Displays the current status for HA.                   |



## APPENDIX A

# Best Practices: Harden Your Cisco EPN Manager Security

---

Security hardening entails making adjustments to ensure that the following components optimize their security mechanisms:

- Cisco EPN Manager web server
- Cisco EPN Manager server
- Cisco EPN Manager storage system (local or external)
- Communication between Cisco EPN Manager and devices
- User authentication system (local or external)
- Time synchronizing system that use Network Time Protocol (NTP)

This appendix will first cover a few core security concepts that administrators should know about. It will then cover the specific tasks that need to be completed in order to optimize Cisco EPN Manager security.

- [Core Security Concepts, on page 743](#)
- [Cisco EPN Manager Security Hardening Overview, on page 745](#)
- [Harden the Cisco EPN Manager Web Server, on page 746](#)
- [Harden the Cisco EPN Manager Server, on page 749](#)
- [Harden Your Cisco EPN Manager Storage, on page 751](#)

## Core Security Concepts

If you are an administrator and are looking to optimize the security of your Cisco EPN Manager product, you should have a good understanding of the following security concepts.

### HTTPS

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) or its subsequent standardization, Transport Layer Security (TLS), to encrypt the data transmitted over a channel. Several vulnerabilities have been found in SSL, so Cisco EPN Manager now supports TLS only.

**Note**

TLS is loosely referred to as SSL often, so we will also follow this convention.

SSL employs a mix of privacy, authentication, and data integrity to secure the transmission of data between a client and a server. To enable these security mechanisms, SSL relies upon certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters.

## SSL Certificates

SSL certificates and private-public key pairs are a form of digital identification for user authentication and the verification of a communication partner's identity. Certificate Authorities (CAs), such as VeriSign and Thawte, issue certificates to identify an entity (either a server or a client). A client or server certificate includes the name of the issuing authority and digital signature, the serial number, the name of the client or server that the certificate was issued for, the public key, and the certificate's expiration date. A CA uses one or more signing certificates to create SSL certificates. Each signing certificate has a matching private key that is used to create the CA signature. The CA makes signed certificates (with the public key embedded) readily available, enabling anyone to use them to verify that an SSL certificate was actually signed by a specific CA.

In general, setting up certificates in both High Availability (HA) and non-HA environments involves the following steps:

1. Generating an identity certificate for a server.
2. Installing the identity certificate on the server.
3. Installing the corresponding root certificate on your client or browser.

The specific tasks you need to complete will vary depending on your environment.

Note the following:

- The start-stop sequencing of servers needs to be done carefully in HA environments.
- Non-HA environments, where a virtual IP address is configured, require the completion of a more complicated certificate request process.

## 1-Way SSL Authentication

This authentication method is used when a client needs assurance that it is connecting to the right server (and not an intermediary server), making it suitable for public resources like online banking websites. Authentication begins when a client requests access to a resource on a server. The server on which the resource resides then sends its server certificate (also known as an SSL certificate) to the client in order to verify its identity. The client then verifies the server certificate against another trusted object: a server root certificate, which must be installed on the client or browser. After the server has been verified, an encrypted (and therefore secure) communication channel is established. At this point, the Cisco EPN Manager server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.



**Note** A client might need to store multiple server certificates to enable interaction with multiple servers.



To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server you want to connect has not been verified. At this point, you can do one of two things: First, you can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field will indicate the certificate was installed successfully. And second, you can install a self-signed certificate on your client. Unlike a root certificate, which is signed by a trusted CA, a self-signed certificate is signed by the person or entity that created it. While you can use a self-signed certificate to create an encrypted channel, understand that it carries an inherent amount of risk because the identity of the server you are connected with has not been verified.

## Cisco EPN Manager Security Hardening Overview

Hardening Cisco EPN Manager security requires completion of the following tasks:

(During installation)

- Configuring HTTPS and setting up 1-way SSL authentication for standalone servers and HA environments
- Shutting down insecure and unused ports
- Configuring network firewalls
- Configuring external authentication

(Post installation)

- Updating certificates in response to changes (like setting a new hostname or IP address)
- Hardening the Cisco EPN Manager server, as needed

Although your primary source of information is your Cisco representative, who can provide server hardening guidance specific to your deployment, you can also follow the steps listed below to secure Cisco EPN Manager

| Hardening Procedure                                                                                   | The procedure hardens:                               |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| <a href="#">Make Web Server Connectivity Secure By Using HTTPS, on page 746</a>                       | Cisco EPN Manager web server                         |
| <a href="#">Set Up Certificate-Based Authentication for Web Clients, on page 746</a>                  |                                                      |
| <a href="#">Configure and Manage OCSP on the Server, on page 749</a>                                  |                                                      |
| <a href="#">Disable Insecure Ports and Services, on page 750</a>                                      | Cisco EPN Manager server                             |
| <a href="#">Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices, on page 607</a> |                                                      |
| <a href="#">Set Up External Authentication Using the CLI, on page 607</a>                             |                                                      |
| <a href="#">Disable Accounts Not Needed for Day-to-Day Operations, on page 751</a>                    |                                                      |
| <a href="#">Harden NTP, on page 610</a>                                                               | Cisco EPN Manager storage system (local or external) |
| <a href="#">Harden Your Cisco EPN Manager Storage, on page 751</a>                                    |                                                      |

## Harden the Cisco EPN Manager Web Server

To harden the Cisco EPN Manager web server, do the following:

1. [Make Web Server Connectivity Secure By Using HTTPS, on page 746](#)
2. [Set Up Certificate-Based Authentication for Web Clients, on page 746](#)
3. [Configure a Custom OCSP Responder on the Server, on page 749](#)

### Make Web Server Connectivity Secure By Using HTTPS

The Cisco EPN Manager web server should be configured to use HTTPS instead of HTTP. This protects the systems that connect to the Cisco EPN Manager web server and also avoids the possibility of any client indirectly intruding into the web server and other participating systems. HTTPS requires using a Certificate Authority (CA) certificate in the web server and appropriate SSL mechanisms. For information on how to set this up, see [Set Up HTTPS to Secure the Connectivity of the Web Server, on page 633](#).

### Set Up Certificate-Based Authentication for Web Clients

For higher-level security, the Cisco EPN Manager server should authenticate clients by using certificate-based authentication. With this form of authentication, Cisco EPN Manager first validates the client's associated certificate to ensure that the client is authentic and then it validates the username and password. This mechanism prevents unauthorized machines (that is, machines for which no certificate exists) to connect with the web server. Cisco EPN Manager implements this feature using the Online Certificate Status Protocol (OCSP).





**Note** The certificate(s) discussed in this topic uniquely identify the *clients*. This is different from the certificate for the *web server*, which was used to set up HTTPS operation. While this procedure is similar to the procedure for generating CER files for web server certificates, it is not exactly the same. You might need to use other tools (such as OpenSSL). In addition, there are different methods for generating CA certificate files. If you need assistance, contact your Cisco representative.

To configure certificate-based authentication:

**Step 1** Generate the client certificate files using a CA, which normally involves the following steps:

- a) Generate the public key.
- b) Generate the CSR file containing the public key.
- c) Submit the CSR file to a CA to get the certificate file(s).
- d) If you receive multiple files, do not concatenate the files to make a single CER/PEM file. Instead:
  - Give the *Client* certificate file to the application user to keep in the client machine.
  - Keep the *Root* and all *Intermediate* CA certificates. You will import them into the server in Step 4.

**Note** You should get these certificates from the root and intermediate CA servers. Do not use any files received from a non-trusted source.

**Note** Do not import the Client CA certificate into the web server. Keep that file with the client machine—for example, on an insertable card, a hardware or software token device, and so forth. When the client browser tries to connect to the Cisco EPN Manager web server, the web server instructs the client browser to ask for the Client certificate. The user must provide the Client certificate, and then enter their username and password.

**Step 2** Log in to the Cisco EPN Manager server using the command line, as explained in [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#). Do not enter config mode.

**Step 3** Enable client certificate authentication on the Cisco EPN Manager web server by running the following command.

```
ncs run client-auth enable
```

This command instructs the web server to enable and use certificate-based client authentication (instead of using usernames and passwords alone).

**Step 4** Import the Root CA and Intermediate CA certificate files, one at a time, into the Cisco EPN Manager web server.

a) Import the Root CA certificate file with this command:

```
ncs key importcacert aliasName rootCACertFile repository repoName
```

Where:

- *aliasName* is the short name supplied for the CA certificate.
- *rootCACertFile* is the Root CA certificate filename.
- *repoName* is the location of the Cisco EPN Manager repository where the certificate file is hosted.

**Note** Note that this command is very different from the command used to apply the server certificate.

b) Import the Intermediate CA certificate file with this command:

```
ncs key importcacert aliasName intermediateCACertFile repository repoName
```

Where:

- *intermediateCACertFile* is the Intermediate CA certificate filename.

**Step 5** Restart the server(s). The procedure you should follow depends on whether your deployment is configured for high availability.

**For deployments *without* high availability**, restart the Cisco EPN Manager server to apply the changes.

```
ncs stop
ncs start
```

**For deployments *with* high availability**, follow these steps, being sure to restart the servers in the correct order.

- a) On the *secondary* server, log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

**Note** Do not restart the secondary server until you reach Step 5(e).

- b) Verify that the secondary server is stopped.  
c) On the *primary* server, log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

**Note** Do not restart the primary server until you reach Step 5(f).

- d) Verify that the primary server is stopped.  
e) On the *secondary* server, run the following commands:
1. Run the **ncs start** command to restart the server.
  2. Verify that the secondary server has restarted.
  3. Run the **ncs status** command and verify that the Health Monitor process is running.
  4. Run the **ncs ha status** command and verify that the HA status of the secondary server is **Secondary Lost Primary**.
- f) On the *primary* server, run the following commands:
1. Run the **ncs start** command to restart the server.
  2. Verify that the primary server has restarted.
  3. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted.

Once all the processes on the primary server are up and running, HA registration is automatically triggered between the secondary and primary servers (and an email is sent to the registered email addresses). This normally completes after a few minutes.

- g) Verify the HA status on the primary and secondary servers by running the **ncs ha status** command on both servers. You should see the following :
- The primary server state is **Primary Active**.

- The secondary server state is **Secondary Syncing**.

---

## Configure and Manage OCSP on the Server

Online Certificate Status Protocol (OCSP) enables certificate-based authentication for web clients using OCSP responders. Typically, the OCSP responder URL is read from the certificate's Authority Information Access (AIA). As a failover mechanism, configure the OCSP responder URL on the Cisco EPN Manager server.

### Configure a Custom OCSP Responder on the Server

To configure a custom OCSP responder URL on the Cisco EPN Manager server:

- 
- Step 1** Log in to the Cisco EPN Manager server using the command line, as explained in [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#). Do not enter config mode.
- Step 2** Enter the following command to enable client certificate authentication:
- ```
ocsp responder custom enable
```
- Step 3** Enter the following command to set the custom OCSP responder URL:
- ```
ocsp responder set url responderNumber responderURL
```

Where:

- *responderNumber* is the number of the OCSP responder you want to define (for example, 1 or 2).
- *responderURL* is the URL of the OCSP responder, as taken from the client CA certificate.

---

### Delete a Custom OCSP Responder from the Server

To delete an existing custom OCSP responder defined on the Cisco EPN Manager server:

- 
- Step 1** Execute the **show security-status** command to view the custom OCSP responders that are currently configured on the server, and identify the number of the responder you want to delete.
- Step 2** Delete the OCSP responder from the server:
- ```
ocsp responder clear url responderNumber
```
- 

## Harden the Cisco EPN Manager Server

Follow these steps to harden the Cisco EPN Manager server.

1. [Disable Insecure Ports and Services, on page 750](#)
2. [Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices, on page 607](#)
3. [Set Up External Authentication Using the CLI, on page 607](#)
4. [Disable Accounts Not Needed for Day-to-Day Operations, on page 751](#)
5. [Harden NTP, on page 610](#)

## Disable Insecure Ports and Services

As a general policy, any ports that are not needed and are not secure should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco EPN Manager for your deployment. You can do this by listing the ports that are open and comparing it with a list of ports that are safe to disable.

You can get this list of ports which are safe to disable from [Cisco Evolved Programmable Network Manager Installation Guide](#), which lists the ports and services used by Cisco EPN Manager.

Follow the procedure below to find out which ports are enabled.

**Step 1** Log in to Cisco EPN Manager using the command line, as explained in [Establish an SSH Session With the Cisco EPN Manager Server, on page 644](#). Do not enter config mode.

**Step 2** The show security-status command displays the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. You will see output similar to the following:

```
show security-status
Open TCP Ports      22 443 1522 8082
Open UDP Ports      162 514 9991
FIPS Mode           enabled
TFTP Service        disabled
FTP Service         disabled
JMS port (61617)    disabled
Root Access         disabled
Client Auth         enabled
OCSP Responder1     http://209.165.200.224/ocsp
OCSP Responder2     http://209.165.202.128/ocsp
```

**Step 3** Check the [Cisco Evolved Programmable Network Manager Installation Guide](#) for the table of ports used by Cisco EPN Manager, and see if your ports are listed in that table. That table will help you understand which services are using the ports, and which services you do not need—and thus can be safely disabled. In this case, *safe* means you can *safely disable the port without any adverse effects to the product*.

**Note** If you are not sure whether you should disable a port or service, contact your Cisco representative.

**Step 4** Disable the insecure ports using the Cisco EPN Manager GUI.

This example disables FTP and TFTP, which are not secure protocols and should be disabled (use SFTP or SCP instead). TFTP and FTP are typically used to transfer firmware or software images to and from network devices and Cisco EPN Manager.

- a) Log in to Cisco EPN Manager with a user ID that has Administrator privileges.
- b) Choose **Administration > Settings > System Settings**, then choose **General > Server**.
- c) Under **FTP** and **TFTP**, select **Disable**, then click **Save**.
- d) Restart Cisco EPN Manager. See [Stop and Restart Cisco EPN Manager, on page 647](#).

- Step 5** If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco EPN Manager to operate. For more information, refer to the [Cisco Evolved Programmable Network Manager Installation Guide](#) (specifically, the information about ports that are used by Cisco EPN Manager and suggested firewall configurations). If you need further help, contact your Cisco representative.
- 

## Disable Accounts Not Needed for Day-to-Day Operations

The Cisco EPN Manager web GUI root user should be disabled after creating at least one other web GUI user that has root privileges. See [Disable and Enable the Web GUI root User, on page 671](#).

## Harden Your Cisco EPN Manager Storage

We recommend that you secure all storage elements that will participate in your Cisco EPN Manager installation, such as the database, backup servers, and so on.

Contact your Cisco representative for more information about hardening your internal or external storage. In the case of external storage, also contact your storage vendor.

If you ever uninstall or remove Cisco EPN Manager, make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted).

## Harden NFS-Based Storage

Since NFS does not have built-in security, you must implement as many of the following security measures as possible to secure the NFS server:

- Set up a firewall in front of the NFS server—To do this practically, tie down the ports that NFS will use in various configuration files and then specify those ports in the firewall configurations.
- Use a port mapper—On the NFS server, only allow NFS transactions that involve specific IP addresses.
- To prevent attacks via a compromised DNS, only specify IP addresses (and not domain names) when configuring NFS.
- When setting up the export of folders, use the **root\_squash** option in the `/etc/exports` file.
- When configuring the `/etc/exports` file, use the **secure** option.
- When configuring the backup staging and storage folders, use the **nosuid** and **noexec** mount options.



---

**Note** It is not mandatory to configure a staging folder.

---

- For the storage folder (and optional staging folder), configure a file access permission value of **755** (which grants all users read and write privileges) and set userid **65534** (the user **nobody**, who does not have any system privileges) as the owner.
- Tunnel NFS traffic either through SSH or SSL/TLS. For SSH, use RSA key-based authentication instead of user authentication.

Do not rely on just one of these measures to secure your NFS-based storage. Your best bet is to implement the combination of measures that best suits your situation. Also keep in mind that this list is not an exhaustive one. To achieve a higher level of confidence when hardening your storage, we recommend that you discuss your situation with a Linux system admin and a security expert beforehand.



## APPENDIX **B**



### Icon and State Reference



- [Device Reachability and Admin States, on page 753](#)
- [Port or Interface States, on page 755](#)
- [Circuit or VC States, on page 756](#)
- [Link Serviceability States, on page 761](#)
- [Link Characteristics, on page 761](#)
- [Equipment Operational States \(Chassis View\), on page 762](#)
- [Alarm Severity Icons, on page 762](#)
- [Device Type Icons, on page 763](#)
- [Circuit or VC Network Topology Overlay Icons, on page 765](#)

### Device Reachability and Admin States

**Device Reachability State**—Indicates whether Cisco EPN Manager can communicate with the device using all configured protocols.





*Table 50: Device Reachability State*

Icon	Device Reachability State	Description	Troubleshooting
	Reachable	Cisco EPN Manager can reach the device using SNMP, or the NCS 2K device using ICMP.	—
	Ping reachable	Cisco EPN Manager can reach the device using Ping, but not via SNMP.	Although ICMP ping is successful, check for all possible reasons why SNMP communication is failing. Check that device SNMP credentials are the same in both the device and in Cisco EPN Manager, whether SNMP is enabled on the device, or whether the transport network is dropping SNMP packets due to reasons such as mis-configuration, etc. See <a href="#">Change Basic Device Properties, on page 271</a> .

	Unreachable	Cisco EPN Manager cannot reach the device using Ping.	Verify that the physical device is operational and connected to the network.
	Unknown	Cisco EPN Manager cannot connect to the device.	Check the device.

**Device Admin State**—Indicates the configured state of the device (for example, if an administrator has manually shut down a device, as opposed to a device being down because it is not reachable by Ping).







**Table 51: Device Admin State**

Icon	Device Admin State	Description	Troubleshooting
	Managed	Cisco EPN Manager is actively monitoring the device.	Not Applicable.
	Maintenance	Cisco EPN Manager is checking the device for reachability but is not processing traps, syslogs, or TL1 messages.	To move a device back to Managed state, see <a href="#">Move a Device To and From Maintenance State, on page 53</a> .
	Unmanaged	Cisco EPN Manager is not monitoring the device.	<p>In the Network Devices table, locate the device and click the "i" icon next to the data in the <b>Last Inventory Collection Status</b> column. The popup window will provide details and troubleshooting tips. Typical reasons for collection problems are:</p> <ul style="list-style-type: none"> <li>• Device SNMP credentials are incorrect.</li> <li>• The Cisco EPN Manager deployment has exceeded the number of devices allowed by its license.</li> <li>• A device is enabled for switch path tracing only.</li> </ul> <p>If a device type is not supported, its Device Type will be <b>Unknown</b>. You can check if support for that device type is available from Cisco.com by choosing <b>Administration &gt; Licenses and Software Updates &gt; Software Update</b> and then clicking <b>Check for Updates</b>.</p>
	Unknown	Cisco EPN Manager cannot connect to the device.	Check the device.







# Port or Interface States



**Port or Interface Primary States**—Conveys the most important state information for a port or interface by combining the admin and operational states. The Multilayer Trace displays either a port's primary state or alarm status. For the Chassis View, if an element does not support the changing of color to indicate a state change, you can still get the state change information from the alarm that is generated.



Port or Interface Primary State	Icon	Admin Status	Operational State
Unknown		Unknown	Unknown
Down		Up	Down
Test		Test	—
Admin Down		Admin Down	—
Up		Up	Up
Auto Up		Up	Auto Up

**Port or Interface Admin Status**—Represents the configured state of the port or interface (for example, if an administrator has manually shut down a port).

Port or Interface Admin Status	Icon	Description
Unknown		Port or interface admin status is unknown. There is no response (or insufficient response) from the device.
Admin Down		Port or interface was manually shut down by the administrator.
Up		Port or interface is enabled by the administrator.
Test		Port or interface is being tested by the administrator.

**Port or Interface Operational State**—Conveys the port or interface's running state and whether it is working properly.

Port or Interface Operational State	Icon	Description
Unknown		Port or interface operational state is unknown. There is no response (or insufficient response) from the device.
Down		Port or interface is not working properly.

Up		Port or interface is receiving and transmitting data.
Auto Up		Port or interface is receiving and transmitting data (only certain devices support this state; other devices use "Up").







## Circuit or VC States

**Circuit or VC Primary States**— Conveys the most important state information for a circuit, in this order: Serviceability, Discovery, Alarm, Provisioning. It is normally shown in the first column of a circuit or VC table.

Circuit or VC Primary State	Icon	Serviceability	Discovery	Alarm	Provisioning
Missing		—	Missing	—	—
Down		Down	—	—	—
Critical		—	—	Critical	—
Major		—	—	Major	—
Minor		—	—	Minor	—
Partially Down		Partial	—	—	—
Admin Down		Admin Down	—	—	—
Partially Discovered		—	Partial	—	—
Failed		—	—	—	(Create, modify, or delete) failed
In progress		—	—	—	(Create, modify, or delete) in progress
Warning		—	—	Warning	—
Up		Up	—	—	—
Auto Up		Auto Up	—	—	—
Info		—	—	Info	—
Cleared		—	—	Cleared	—

**Circuit or VC Serviceability State**— This value is a combination of the circuit or VC's admin and operational states. The admin state is shown because it impacts service operability. For optical circuits, the admin state

also determines whether the Activate and Deactivate actions are available. The operational state is shown to quickly identify whether a service is working or not.

Circuit or VC Serviceability State	Icon	Description
Admin Down		Circuit or VC manually shut down by the administrator.
Down		Circuit or VC is operationally down and administratively up.
Up		Circuit or VC is operationally and administratively up.
Auto Up		Circuit or VC is operationally auto up and administratively up. Only certain devices support the Auto Up operational state.
Unavailable		Circuit or VC has not been discovered yet, or its operational status is unavailable.
Partial		<p>Circuit/VC operational or administrative state is partial.</p> <ul style="list-style-type: none"> <li>• Partial admin state—The circuit or VC has a mixed administrative request (to activate some service resources and deactivate others), has a mix of resources that are administratively up and down, or has resources whose operational state is unavailable.</li> <li>• Partial operational state—The circuit or VC has a mix of some active and deactivated resources, or the operational state for some of its resources are unavailable.</li> </ul>

Following table provides details of the serviceability states of Circuits/VCs under various scenarios:




Technology	Service Type	Scenario	Serviceability State
------------	--------------	----------	----------------------

Carrier Ethernet	EPL, EVPL, Access EPL, and Access EVPL	If the operational state of the endpoints (service instance / sub-interface), cross connects, and pseudowire participating in the service is up	Up
		If the admin state of both, the source and destination endpoints (service instance / sub-interface) participating in the service is down	Admin Down
		In all the other scenarios, when at least one endpoint (service instance / sub-interface), cross connect, or the pseudowire participating in the service is down	Down
	EP-LAN, EVP-LAN, EP-Tree, and EVP-Tree	If all the endpoints (service instance / sub-interface), bridge domains, VFIs, and pseudowires participating in the service are up	Up
		If the operational state of at least two endpoints (service instance / sub-interface) participating in the service are up and the rest of the endpoints are down	Partial
		If the admin state of all the endpoints (service instance / sub-interface) participating in the service is down	Admin Down
		If the operational state of at least one endpoint (service instance / sub-interface) participating in the service is up and the rest of the endpoints are down	Down


Circuit Emulation	All service types	If the operational state of the endpoints (cemGroup), underlying TDM controller, cross connect, and pseudowire participating in the service are up	Up
		If the admin state of both, the source and destination endpoints (cemGroup) participating in the service is down	Admin Down
		In all the other scenarios, when the operational state of one of the endpoint (cemGroup), underlying TDM controller, cross connect, and pseudowire participating in the service is down	Down
MPLS	Unidirectional TE Tunnel	If the operational state of the tunnel interface is up	Up
		If the admin state of the tunnel interface is down	Admin Down
		In all the other scenarios, when the operational state of the tunnel is down	Down
	Bidirectional TE Tunnel	If the operational states of the interfaces on both ends of the tunnel is up	Up
		If the admin states of the interfaces on both ends of the tunnel is down	Admin Down
		In all the other cases, when the operational state of the tunnel interface is down	Down





Layer 3 VPN		If the operational state of all the endpoints (sub-interface, BDI, and BVI) participating in the service is up	Up
		If the operational state of at least two endpoints (sub-interface, BDI, and BVI) participating in the service are up and the rest of the endpoints are down	Partial
		If the admin state of all the endpoints (sub-interface, BDI, and BVI) participating in the service is down	Admin Down
		If the operational state of at least one endpoint (sub-interface, BDI, and BVI) participating in the service is up and the rest of the endpoints are down	Down

**Circuit or VC Discovery State**—Represents the latest state and structure of a service and its components, as discovered from the network. Having a Discovered version means that the application is actually monitoring the service itself, e.g. it can define meaningful operational and performance data.







Circuit or VC Discovery State	Icon	Description
Partial		Circuit or VC partially discovered by Cisco EPN Manager ; not all of its expected entities have been discovered.
Full		Circuit or VC fully discovered by Cisco EPN Manager , so Cisco EPN Manager can monitor the service and provide meaningful operational and performance data.
Missing		Circuit or VC not yet discovered by Cisco EPN Manager (though it may have been provisioned).

**Circuit or VC Provisioning State**—Represents whether there is a provisioning intent for a circuit or VC and, if so, its status. If a reconciliation report has been generated, the state of the reconcile action is reflected.

Circuit or VC Provisioning State	Icon	Description
None		Circuit or VC was discovered but has not yet been provisioned. The circuit/VC must be promoted in order to modify or delete it.

Failed		Action has failed.
In Progress		Action was initiated but not yet completed.
Planned		Action is planned but not yet initiated.
Succeeded		Action has completed successfully.

## Link Serviceability States

Serviceability State	Icon	Description
Admin Down		Link was purposefully shut down by the administrator.
Down		Link is down (but it should not be).
Up		Link is up and traffic is passing through the link.
Auto Up		Link is up because it detected a signal (this state is only supported by optical devices).
Unavailable		Link is not discovered yet or its status is unavailable.
Partial		Link has a mismatch between requests, resources, or resource states. Examples: <ul style="list-style-type: none"> <li>• Link is processing a request to activate some service resources and deactivate others.</li> <li>• Link has some active and some deactivated resources.</li> <li>• Some link resources are up and others are down.</li> <li>• The state for one of the link's resources is not known.</li> </ul>

## Link Characteristics

The following table describes the different types of links used to represent the connection between devices in the Topology Map view of Cisco EPN Manager .

Link Type	Description
-----------	-------------

	<p><b>Solid Line</b>—Indicates a physical, topological, or service link, such as a link between two devices.</p>
	<p><b>Dashed Line</b>—Indicates an association or business link between elements such as EVCs, VPLS service instances, or VPN components.</p>

## Equipment Operational States (Chassis View)

The equipment operational states represent the running state of the network element.

Equipment Operational State	Icon	Description
In Service	(none)	Equipment is operating properly.
Pre-provisioned		(Cisco NCS 2000 and Cisco ONS devices only) Equipment has been configured but is not physical present in the chassis.
Failed/Disabled/Down/Out of Service/Out of Service Maintenance		Equipment is not operating properly.
Unknown		Equipment operational state is unknown. No response (or insufficient response) from the device.

## Alarm Severity Icons

The table below lists the alarm colors and their respective severity levels for the icons displayed in various parts of the web GUI.






Severity Icon	Description	Color
	Critical alarm	Red















Severity Icon	Description	Color
	Major alarm	Orange
	Minor alarm	Yellow
	Warning alarm	Light Blue
	Alarm cleared; normal, OK	Green
	Informational alarm	Medium Blue
	Indeterminate alarm	Dark Blue

## Device Type Icons









Table below defines the icons used to represent different device types in the Topology and the Multi-layer Trace views in Cisco EPN Manager .





Icon	Definition
	Switch
	Router
	Router Aggregated
 	<p>Cisco NCS 6000 device on which a Secure Domain Router (SDR) resides. The SDR's name is listed directly above the device's icon.</p> <p><b>Note</b> There may be cases where the SDR label for a device that belongs to a cluster or user-defined group is not displayed (since auto-clustering is applied to devices based on their proximity).</p>

Icon	Definition
	Router configured with an L3VPN service.
	Switch Aggregated
	Access Point
	Service Module
	UCS C-Series
	NAM Blade
	Group
	Generic Device
	Virtual Server
	Wireless LAN Controller

Icon	Definition
	Unknown
	DWDM ROADM Regeneration/NCS 2000

## Circuit or VC Network Topology Overlay Icons

Overlay Icon	Definition
	Source endpoint
	Destination endpoint
	EVC or CEM service with local switching
	Endpoint included by the user during creation of the circuit.
	Endpoint excluded by the user during the creation of the circuit.
	Endpoint with some ports that were either included or excluded during creation of the circuit. This endpoint contains multiple ports that are participating in various routes of the circuit.
	E-TREE EVC endpoint that has been designated as a root.
	Selected endpoint.

Overlay Icon	Definition
	Hub; If the hub and root are on the same device (VPLS scenario), the brown circle is combined with the root icon.
	Link included during creation of the circuit.
	Link excluded during creation of the circuit.
	Endpoint with some ports that were either included or excluded during creation of the circuit. This represents the aggregated link that contains multiple ports participating in various routes of the same circuit.



## APPENDIX C

# Monitoring Policies Reference

The following topics describe the monitoring policies used by Cisco EPN Manager . For information on the supported MIBs and MIB objects, see [Cisco Evolved Programmable Network Manager Supported Devices](#).

- [Device Health Monitoring Policy, on page 767](#)
- [Interface Health Monitoring Policy, on page 768](#)
- [Custom MIB Polling Monitoring Policy, on page 768](#)
- [IP SLA Y.1731 Monitoring Policy, on page 768](#)
- [Pseudowire Emulation Edge to Edge Monitoring Policy, on page 769](#)
- [Quality of Service Monitoring Policy, on page 769](#)
- [IP SLA Monitoring Policy, on page 770](#)
- [ME1200 EVC QoS Monitoring Policy, on page 770](#)
- [BNG Sessions and IP Pools Monitoring Policy, on page 771](#)
- [TDM/SONET Ports Monitoring Policy, on page 771](#)
- [Optical SFP Monitoring Policy, on page 771](#)
- [Optical 1 Day and Optical 15 Mins Monitoring Policies, on page 772](#)
- [CEM Monitoring Policy, on page 772](#)
- [Device Sensor Monitoring Policy, on page 773](#)
- [Performance Counters for Optical Monitoring Policies, on page 773](#)

## Device Health Monitoring Policy

The Device Health Monitoring Policy monitors device CPU utilization, memory pool utilization, environmental temperature, and device availability for all devices in the network. By default, the policy polls devices for this information every 5 minutes, and an alarm is generated if CPU utilization, memory pool utilization, or environmental temperature thresholds are surpassed.

This monitoring policy is activated by default after installation.



### Note

This policy does not monitor the device CPU utilization and memory pool utilization for supported Cisco ONS or Cisco NCS 2000 devices, but it does monitor memory utilization and device availability.

For information on how to manage this policy, see [Set Up Basic Device Health Monitoring, on page 194](#).

# Interface Health Monitoring Policy

An Interface Health Monitoring Policy monitors over 30 attributes to check interface operational status and performance. It polls device interfaces every 5 minutes and generates an alarm when interface discard, error, utilization, or byte rate thresholds are exceeded.

To protect the performance of large deployments, this policy is not activated by default.

Note the following:

- This policy does not monitor optical interfaces. Use an optical policy to monitor that information. See [Optical 1 Day and Optical 15 Mins Monitoring Policies, on page 772](#).
- Due to a limitation in this release, you cannot retrieve and view cyclic redundancy check (CRC) error data for the interfaces associated with a particular port group from either the Network Summary dashboard's **Top N Interface CRC Errors** dashlet or a REST API call.

See these topics for information on how to manage this policy:

- To check whether an Interface Health policy is actively monitoring interfaces, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To set up interface monitoring, see [Set Up Basic Interface Monitoring, on page 195](#).
- To adjust an interface monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

# Custom MIB Polling Monitoring Policy

The Custom MIB Polling monitoring policy is a customizable policy you can use to monitor unsupported parameters—that is, parameters that are not polled by any of the existing monitoring policy types. When you create a Custom MIB Polling policy, you can choose from an extensive list of Cisco and other MIBs, or import new MIBs into the policy. If a Custom MIB Polling policy is collecting device performance information, you can display that data in the Performance dashboard by creating a generic dashlet (see [Add a Customized Dashlet to the Device Trends Dashboard, on page 22](#)). For more information on managing Custom MIB Polling monitoring policies, see the following topics:

- To check if a Custom MIB Polling policy is being used to monitoring information, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new Custom MIB Polling policy, see [Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 203](#).
- To adjust an existing Custom MIB Polling policy, see [Adjust What Is Being Monitored, on page 201](#).

# IP SLA Y.1731 Monitoring Policy

An IP SLA Y.1731 monitoring policy uses the Y.1731 ITU-T recommendation to monitor over 70 fault and performance attributes in Metro Ethernet networks. When you create an IP SLA Y.1731 monitoring policy, it polls the parameters every 15 minutes and generates an alarm when delay, jitter, frame loss, and other thresholds are exceeded.

For more information on how to configure and manage an IP SLA Y.1731 monitoring policy, see these topics:

- To check if IP SLA Y.1731 parameters are being monitored, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new IP SLA Y.1731 monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing IP SLA Y.1731 monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

## Pseudowire Emulation Edge to Edge Monitoring Policy

A Pseudowire Emulation Edge to Edge (PWE3) monitoring policy polls approximately 20 attributes that emulate edge-to-edge services over a Packet Switched Network (PSN). When you create and enable a monitoring policy that uses this policy type, attributes are polled every 15 minutes by default. In addition, Cisco EPN Manager generates a minor alarm when the thresholds for the following attributes are surpassed on pseudowire virtual circuits (PW VCs):

- HC packets and bytes—Total in and total out rates
- Operational status up, inbound and outbound operational status up

For more information on how to configure and manage a PWE3 monitoring policy, see these topics:

- To check if PWE3 parameters are being monitored, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new PWE3 monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing PWE3 monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

## Quality of Service Monitoring Policy

A Quality of Service monitoring policy polls over 60 service parameters to validate the quality of services running on network devices. When you create a Quality of Service monitoring policy, it polls the parameters every 15 minutes and generates an alarm when certain thresholds are exceeded. The following is a partial list of parameters that can cause an alarm:

- Dropped/discarded bytes and packets rates
- Pre-policy bytes and packets rates, utilization, percent of Committed Information Rate (CIR), Peak Information Rate (PIR)
- Post-policy bytes rates, utilization, percent of Committed Information Rate (CIR), Peak Information Rate (PIR)

To view all Quality of Service parameters that can cause TCAs, see [Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 200](#).

For more information on how to configure and manage a Quality of Service monitoring policy, see these topics:

- To check if Quality of Service parameters are being monitored, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).

- To create a new Quality of Service monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing Quality of Service monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

## IP SLA Monitoring Policy

An IP SLA monitoring policy monitors approximately 20 parameters to provide real-time performance information. When you create an IP SLA monitoring policy, it polls the parameters every 15 minutes. This monitoring policy does not generate any alarms; if you want to generate IP SLA-based alarms, use the IP SLA Y.1731 monitoring policy.

For more information on how to configure and manage an IP SLA monitoring policy, see these topics:

- To check if IP SLA parameters are being monitored, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new IP SLA monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing IP SLA monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

## ME1200 EVC QoS Monitoring Policy

A ME1200 QoS monitoring policy polls over 20 service parameters to validate the quality of selected services running on ME1200 devices. When you create a ME1200 Quality of Service monitoring policy, it polls the parameters every 15 minutes but does not generate an alarm when certain thresholds are exceeded. The following is a partial list of parameters that are polled by ME1200 QoS monitoring policy:

- Transmitted and discarded bytes and packets rates.
- Average bit and frame rates for green (conforming), yellow (exceeding), red (violating), and discard traffic (both inbound and outbound).

To view all ME1200 QoS parameters that are polled, see [Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 200](#).

For more information on how to configure and manage a ME1200 QoS monitoring policy, see these topics:

- To check if ME1200 QoS parameters are being monitored, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new ME1200 QoS monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing ME1200 QoS monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).



## BNG Sessions and IP Pools Monitoring Policy

This monitoring policy polls over 5 parameters to monitor the BNG sessions as well as the IP addresses leased from the IP pools. When you create a BNG Sessions and IP Pools monitoring policy, it polls the parameters every 15 minutes and generates an alarm when certain thresholds are exceeded. The following is a partial list of parameters that can cause an alarm:

- Number of used or free IP addresses in the IP pools.
- Number of sessions for authenticated and up subscribers.

To view all BNG Sessions and IP Pools parameters that can cause TCAs, see [Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 200](#).

For more information on how to configure and manage a BNG Sessions and IP Pools monitoring policy, see these topics:

- To check if BNG Sessions and IP Pools parameters are being monitored , see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new BNG Sessions and IP Pools monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing BNG Sessions and IP Pools monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

## TDM/SONET Ports Monitoring Policy

The TDM/Sonet Ports monitoring policy monitors approximately 20 circuit emulation (CEM) parameters. When you create a TDM/SONET Ports monitoring policy, it polls the CEM parameters every 15 minutes and generates an alarm when errored seconds (ES), unavailable sessions (UAS), and code violation (CV) thresholds are exceeded.

For more information on how to configure and manage a TDM/SONET Ports monitoring policy, see these topics:

- To check if TDM/SONET Ports parameters are being monitored , see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new TDM/SONET Ports monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing TDM/SONET Ports monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

## Optical SFP Monitoring Policy

An Optical SFP monitoring policy polls health and performance information for optical small form-factor (SFP) interfaces. This policy polls temperature, voltage, current, and optical TX/RX power. When you create an Optical SFP monitoring policy, it polls the parameters every 1 minute.

For more information on how to configure and manage an Optical SFP monitoring policy, see these topics:

- To check if Optical SFP parameters are being monitored, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new Optical SFP monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing Optical SFP monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

## Optical 1 Day and Optical 15 Mins Monitoring Policies

The Optical 1 Day and Optical 15 Mins monitoring policies poll the following optical interfaces:

- Physical, OTN, Ethernet, and SONET/SDH interfaces on Cisco NCS 4000 devices
- DWDM interfaces on Cisco NCS 2000 and Cisco ONS devices

Device availability and environmental temperature is monitored by the Device Health monitoring policy. See [Device Health Monitoring Policy, on page 767](#) for more information.

See [Performance Counters for Optical Monitoring Policies, on page 773](#) for a list of the parameters that these policies poll.

For more information on how to configure and manage an Optical 1 Day and Optical 15 Mins monitoring policy, see these topics:

- To check if Quality of Service parameters are being monitored, see [Check What Cisco EPN Manager Is Monitoring, on page 198](#).
- To create a new Quality of Service monitoring policy, see [Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 203](#).
- To adjust an existing Quality of Service monitoring policy, see [Adjust What Is Being Monitored, on page 201](#).

## CEM Monitoring Policy

Use the CEM Monitoring Policy to poll the following CEM parameters:

- Jitter Buffer Overruns
- Generated Lbits
- Received Lbits
- Generated Rbits
- Received Rbits
- Generated Nbits
- Received Nbits
- Generated Pbits

- Received Pbits

The polling happens through the CLI and the delta of the current and last collection is taken as the current entry.



**Note** This polling data is not displayed in the dashboard.

## Device Sensor Monitoring Policy

Use the Device Sensor monitoring policy to poll the sensor information through SNMP to the devices that are added to this policy. The sensor details such as voltage, power, and current temperature are polled to the device.



**Note** There are no calculations involved in the device sensor data.

## Performance Counters for Optical Monitoring Policies

The following topics list the performance counters used by the optical monitoring policies. This information is provided here because it is not available from the web GUI.

- [Reference—Performance Counters for Physical Interfaces, on page 773](#)
- [Reference—Performance Counters for OTN-FEC Interfaces, on page 775](#)
- [Reference—Performance Counters for OTN-ODU Interfaces, on page 775](#)
- [Reference—Performance Counters for OTN-OTU Interfaces, on page 776](#)
- [Reference—Performance Counters for Ethernet Interfaces, on page 777](#)
- [Reference—Performance Counters for SONET Interfaces, on page 779](#)
- [Reference—Performance Counters for SDH Interfaces, on page 779](#)

## Reference—Performance Counters for Physical Interfaces

The following table lists the performance counters used by the optical policy types to monitor physical interfaces.

Performance counters marked with an asterisk (\*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices. Performance counters marked with a double asterisk (\*\*) are applicable for Cisco Network Convergence System (NCS) 4000 series devices.

Physical Interface Performance Counter	Description
----------------------------------------	-------------

OPR-MIN	Minimum output power received by the optical circuit.
OPR-AVG	Average output power received by the optical circuit.
OPR-MAX	Maximum output power received by the optical circuit.
OPT-MIN	Minimum output power transmitted from the optical circuit.
OPT-AVG	Average output power transmitted from the optical circuit.
OPT-MAX	Maximum output power transmitted from the optical circuit.
LBC-MIN* LBCL-MIN	Minimum laser bias current for the optical circuit.
LBC-AVG* LBCL-AVG	Average laser bias current for the optical circuit.
LBC-MAX* LBCL-MAX	Maximum laser bias current for the optical circuit.
DGD-MIN**	Minimum differential group delay for the optical circuit.
DGD-AVG**	Average differential group delay for the optical circuit.
DGD-MAX**	Maximum differential group delay for the optical circuit.
SOPMD-MIN**	Minimum second order polarization mode dispersion for the optical circuit.
SOPMD-AVG**	Average second order polarization mode dispersion for the optical circuit.
SOPMD_MAX**	Maximum second order polarization mode dispersion for the optical circuit.
OSNR-MIN**	Minimum optical signal to noise ratio for the optical circuit.
OSNR-AVG**	Average optical signal to noise ratio for the optical circuit.
OSNR-MAX**	Maximum optical signal to noise ratio for the optical circuit.
PDL-MIN**	Minimum polarization dependent loss for the optical circuit.
PDL-AVG**	Average polarization dependent loss for the optical circuit.
PDL-MAX**	Maximum polarization dependent loss for the optical circuit.
PCR-MIN**	Minimum polarization change rate for the optical circuit.
PCR-AVG**	Average polarization change rate for the optical circuit.
PCR-MAX**	Maximum polarization change rate for the optical circuit.
PMD-AVG*,**	Average polarization mode dispersion for the optical circuit.

PMD-MIN*,**	Minimum polarization mode dispersion for the optical circuit.
PN-MIN**	Minimum phase noise for the optical circuit.
PN-AVG**	Average phase noise for the optical circuit.
PN-MAX**	Maximum phase noise for the optical circuit.
PREFEC-BER*	Pre-forward error correction bit error rate for the optical circuit.
CD-MIN**	Minimum chromatic dispersion for the optical circuit.
CD-AVG**	Average chromatic dispersion for the optical circuit.
CD-MAX**	Maximum chromatic dispersion for the optical circuit.

## Reference—Performance Counters for OTN-FEC Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-FEC interfaces.

Performance counters marked with an asterisk (\*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices.

OTN-FEC Interface Performance Counter	Description
BIT-EC* BIEC	Number of bit errors corrected.
UNC-WORDS* UCW	Number of uncorrectable words.

## Reference—Performance Counters for OTN-ODU Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-ODU interfaces.

OTN-ODU Interface Performance Counter	Description
BBE-PM	Number of background block errors in path monitoring.
BBER-PM	Background block errors ratio in path monitoring.
ES-PM	Number of errored seconds in path monitoring.
ESR-PM	Errored seconds ratio in path monitoring.
SES-PM	Number of severely errored seconds in path monitoring.
SESR-PM	Severely errored seconds ratio in path monitoring.

UAS-PM	Number of unavailable seconds in path monitoring.
FC-PM	Number of failure counts (AIS/RFI detected) in path monitoring.
gfpStatsRxFrames	Number of generic framing procedure (GFP) frames received.
gfpStatsTxFrames	Number of GFP frames transmitted.
gfpStatsRxOctets	Number of GFP bytes received.
gfpStatsTxOctets	Number of GFP bytes transmitted.
gfpStatsRxCRCErrors	Number of packets received with a payload frame check sequence (FCS) error.
gfpStatsRxMBitErrors	Number of multiple bit errors. In the GFP core header at the GFP-transparent (GFP-T) receiver, these are uncorrectable.
gfpStatsRxSBitErrors	Number of single bit errors. In the GFP core header at the GFP-T receiver, these are correctable.
gfpStatsRxTypeInvalid	Number of packets received with invalid GFP type. This includes unexpected user payload identifier (UPI) type and errors in core header error check (CHEC).
gfpStatsRxCIDInvalid	Number of packets received with invalid CID.
gfpStatsRoundTripLatencyUsec	Round trip delay for the end-to-end Fibre Channel transport in milliseconds.
gfpStatsTxDistanceExtBuffers	Number of buffer credit transmitted for GFP-T transmitter (valid only if distance extension is enabled).
gfpStatsRxSblkCRCErrors	Number of super block cyclic redundancy check (CRC) errors.
gfpStatsCSFRaised	Number of GFP client signal fail (CSF) frames detected at the GFP-T receiver.
gfpStatsLFDRaised	Number of GFP loss of frame delineation (LFD) detected.
gfpRxCmfFrame	Number of client management frames (CMF) received.
gfpTxCmfFrame	Number of client management frames (CMF) transmitted.
gfpStatsCHecRxMBitErrors	Number of core header error control (cHEC) CRC multiple bit errors.
gfpStatsTHecRxMBitErrors	Number of type header error control (tHEC) CRC multiple bit errors.

## Reference—Performance Counters for OTN-OTU Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-OTU interfaces.

OTN-OTU Interface Performance Counter	Description
BBE-SM	Number of background block errors in section monitoring.
BBER-SM	Background block error ratio in section monitoring.
ES-SM	Number of errored seconds in section monitoring.
ESR-SM	Errored seconds ratio in section monitoring.
SES-SM	Number of severely errored seconds in section monitoring.
SESR-SM	Severely errored seconds ratio in section monitoring.
UAS-SM	Number of unavailable seconds in section monitoring.
FC-SM	Number of failure counts (AIS/RFI detected) in section monitoring.

## Reference—Performance Counters for Ethernet Interfaces

The following table lists the performance counters used by the optical policy types to monitor Ethernet interfaces.

Ethernet Interface Performance Counter	Description
ifInOctets	The total number of octets received on the interface, including framing octets.
ifInErrors	The total number of received packets that were discarded because of errors.
ifOutOctets	The total number of transmitted octets, including framing packets.
ifInUcastPkts	The total number of unicast packets received since the last counter reset.
ifOutUcastPkts	The total number of packets requested by the higher-level protocols to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifInMulticastPkts	The total number of multicast packets received since the last counter reset.
ifOutMulticastPkts	The total number of multicast frames transmitted error free.
ifInBroadcastPkts	The total number of broadcast packets received since the last counter reset.
ifOutBroadcastPkts	The total number of packets requested by higher-level protocols and addressed to a broadcast address at this sublayer, including those that were not transmitted.
txTotalPkts	The total number of packets transmitted.
rxTotalPkts	The total number of packets received.

etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed. Note that for tagged interfaces, this number becomes 1522 bytes.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size.
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts512to1023Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.



## Reference—Performance Counters for SONET Interfaces

The following table lists the performance counters used by the optical policy types to monitor SONET interfaces.

Performance counters marked with an asterisk (\*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices.

<b>SONET Interface Performance Counter</b>	<b>Description</b>
CV-S* CVS	Number of coding violations per section.
ES-S* ESS	Number of errored seconds per section.
SES-S* SESS	Number of severely errored seconds per section.
SEFS-S* SEFSS	Number of severely errored frame seconds per section.
CV-L* CVL	Number of coding violations per line for near end and far end devices.
ES-L* ESL	Number of errored seconds per line for near end and far end devices.
SES-L* SESL	Number of severely errored seconds per line for near end and far end devices.
UAS-L* UASL	Number of unavailable seconds per line for near end and far end devices.
FC-L* FCL	Number of failure counts per line for near end and far end devices.

## Reference—Performance Counters for SDH Interfaces

The following table lists the performance counters used by the optical policy types to monitor SDH interfaces.

<b>SDH Interface Performance Counter</b>	<b>Description</b>
MS-ES	Number of errored seconds per multiplex section for near end and far end devices.

MS-ESR	Error seconds ratio per multiplex section for near end and far end devices.
MS-SES	Number of severely errored seconds per multiplex section for near end and far end devices.
MS-SESR	Severely errored seconds ratio per multiplex section for near end and far end devices.
MS-BBE	Number of background block errors per multiplex section for near end and far end devices.
MS-BBER	Background block error ratio per multiplex section for near end and far end devices.
MS-UAS	Number of unavailable seconds per multiplex section for near end and far end devices.
MS-EB	Number of errored block per multiplex section for near end and far end devices.
MS-FC	Number of failure counts per multiplex section for near end and far end devices.
MS-PSC	Protection switching count per multiplex section. PSC is the number of times the service switches from a working card to a protection card and back.
MS-PSC-R	Protection switching count ring per multiplex section. This count is incremented only if ring switching is used.
MS-PSC-S	Protection switching count span per multiplex section. This count is incremented only if span switching is used.
MS-PSC-W	Protection switching count working per multiplex section. It is the count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line.
MS-PSD	Protection switching duration applies to the length of time, in seconds, that service is carried on another line.
MS-PSD-R	Protection switching duration ring is a count of the seconds that the protection line was used to carry service. This count is incremented only if ring switching is used.
MS-PSD-S	Protection switching duration span is a count of the seconds that the protection line was used to carry service. This count is incremented only if span switching is used.
MS-PSD-W	Protection switching duration working per multiplex section.
RS-ES	Number of errored seconds per regenerator section.
RS-ESR	Errored seconds ratio per regenerator section.
RS-SES	Number of severely errored seconds per regenerator section.
RS-SESR	Severely errored seconds ratio per regenerator section.
RS-BBE	Number of background block errors per regenerator section.
RS-BBER	Background block errors ratio per regenerator section.
RS-UAS	Number of unavailable seconds per regenerator section.

RS-EB	Number of errored block per regenerator section.
RS-OFS	Number of out-of-frame seconds per regenerator section.

